NHSmail: Data Retention and Information Management Policy

November 2022
Version 10

Revision History

Version	Date	Summary of Changes
V4	January 2020	Update to inactive shared mailbox section – sending email in last six months.
V5	October 2020	Update to data retention definition section – availability of Exchange Online and O365 retention guidance.
V8	August 2021	Removal of reference to 'dummy mailbox' option from forensic process as this is not an option. Addition of detail that reuse of email addresses is not possible.
V9.1	September 2022	Update to Inactive person accounts and Deleted accounts - Update to Inactive person accounts and Deleted accounts - Accounts that have the auto-expanding archive mailbox feature enabled cannot be recovered or restored. To recover an auto-expanding archive mailbox, a service request will have to be made for a forensic extract on the account
V10	November 2022	Update to account management lifecycle to reduce active and inactive periods from 90 to 30 days. The period prior to deletion for new accounts that have not accepted the AUP and set security questions has also reduced from 90 to 30 days.

Contents

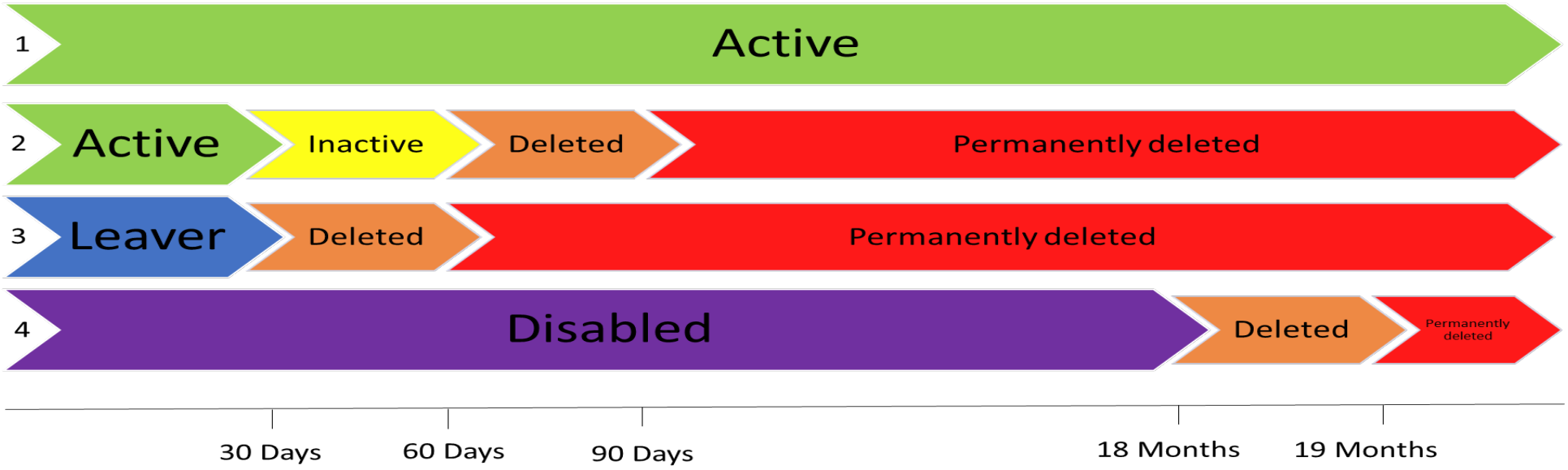
Introduction

This document defines the data retention and information management approach for the NHSmail service and the minimum retention periods for which data will be kept.

The document provides a description of the types of data and the account management lifecycle. A full breakdown of the retention periods is given in the data retention definition section.

Account management lifecycle

User accounts go through a defined lifecycle, as described below:



1. Relates to active accounts that are regularly used i.e., Accessed their account at least once every 30 days to remain active. Please note this could be any 365 service such as MS Teams or SharePoint account. Accounts that are used purely via delegation will not prevent the account transitioning into an inactive state. To prevent this from occurring, accounts should be accessed via the Outlook client or by OWA using the associated login credentials. It should also be noted that a password reset performed on an account must be performed by the account owner logging in via the NHSmail Portal. Password resets performed on behalf of an account owner by a Primary Local Administrator or Local Administrator will not contribute to keeping an account active.

2. Relates to active accounts that are NOT regularly used i.e. An account that is not accessed at least once every 30 days. Please note this could be any 365 service such as MS Teams or SharePoint account. For accounts that are not regularly used they will become inactive after 30 days and then remain in a state of inactive for a further 30 days. After this period, the account will be eligible for deletion via the account hygiene process.

3. An active account that has been set as a ‘leaver’ by an organisation’s Local Administrator (LA). If the account is not joined to a new organisation within 30 days, it will become eligible for deletion. The account will be eligible for permanent deletion after another 30 days.

4. A disabled (formerly suspended) account can remain in the ‘disabled’ status for a maximum of 18 months. If the status remains unchanged after this 18month period the account will be deleted, and any residual data securely erased. The account will be eligible for permanent deletion after another 30 days. Note: For data retention and information please see the below documentation. Data Retention and Information Management Policy.

Account status and retention period

Account status	Account retention period	Additional detail
Active accounts	Retained indefinitely whilst the account is active.	An account will remain active if at least one of the following actions is taken within the last 30 days: • Logging into the NHSmail portal • Logging into an NHSmail shared tenant O365 application (e.g., Teams) • Use of O365 applications (e.g., Outlook with cached credentials) • Sending an email Information on self-service password management and changing your password can be found on the NHSmail support site.
Inactive person accounts	Retained within the service for 30 days	Relates to active accounts that are NOT regularly used i.e., an account that is not logged into for 30 days. For accounts that are not regularly used they will become inactive after 30 days and then remain in an inactive state for a further 30 days. After this period, the account will be eligible for deletion via the account hygiene process. Accounts that have the auto-expanding archive mailbox feature enabled cannot be recovered or restored. To recover an auto-expanding archive mailbox, a service request will have to be made for a forensic extract on the account. This will trigger a process to begin recovering these items.

Accounts marked as a 'leaver' by a Local administrator (LA)	Remains in use for 30 days after which it will be deleted, unless joined to another organisation.	Accounts must be marked as a 'leaver' by the LA when a user leaves an organisation. The account holder then has 30 days to get the account 'joined' to a new organisation. If this action is not completed, the account and data within will be deleted. Deleted accounts cannot be restored after 30 days. For guidance on how to find your LA, see the guidance Finding your Local Administrator. For pharmacy, social care and dentistry users, the LA responsibilities are carried out by the National Administration Service (NAS). Data relating to the current organisation should be managed in line with local information governance policies and processes. It is recommended any data relating to the current organisation is removed by the LA and mailbox owner prior to the account being marked as a 'leaver.' For further information on managing accounts of users leaving the organisation please see the Leavers and Joiners guide.

Account status	Account retention period	Additional detail
Inactive shared mailboxes	Removed after a specified period	Shared mailboxes that have not sent mail for over 6 months, will be identified via communications sent to the mailbox owner and deleted after a specified period.
Disabled accounts	Removed 18 months after the date the LA disabled the account.	Accounts that have disabled status will be automatically deleted 18 months after the date the LA disabled the account, if no further changes have been made to their status, such as re-enabling.
Deleted accounts	Removed 1 month (30 days) after deletion.	Once an account has been deleted, it is recoverable through the NHSmail Portal for 30 days. Deleted accounts cannot be recovered after 30 days. **Note:** Unlike other deleted accounts, accounts that have the auto-expanding archive mailbox feature enabled cannot be recovered through the NHSmail Portal after deletion. To recover an auto-expanding archive mailbox, a service request will have to be made for a forensic extract on the account. This will trigger a process to begin recovering these items.
Newly created accounts that have not been activated	30 days from date of creation.	Accounts that are registered by LAs but not activated by a user (accepting the AUP and creating security questions and answers) will be removed after 30 days.
Application accounts	Retained indefinitely whilst the account is active.	An account will remain active if it has been logged into, or had a password change, or sent an email within the last 12 months.

Note: For any account that is deleted from use, data remains available for forensic investigations as per the data retention timeframes detailed in the data retention definition section.

Ways of accessing data

Area	Description
Audit report	To view and understand what activities have taken place by an LA or user, in the Portal. This is available by self-service in the Portal for LAs – please refer to the Auditing Actions.
Forensic investigations	This information is only available for 'forensic' searches (for example, HR, criminal, clinical) initiated by the organisation's HR director / CEO for which the account resides in at the time of request. Please see the Access to Data Procedure for guidance on how to request access to NHSmail data, for the purpose of official investigations. A mailbox snapshot is provided to allow the requestor a full copy of the user's mailbox at the time of the request being processed.
Directory / mailbox data	End-user can access and make changes, as necessary.

Note: When data is recovered on behalf of an organisation, there are no guaranteed times to return data and requests are processed on a first come, first served basis. No attempt will be made to prioritise requests.

Data retention definition

Important note: All retention definition material included below relates to users currently residing in Exchange On-Premise. For Exchange Online and O365 retention information, please see Data Retention and Information Management Policy – Office 365 – NHSmail Support

Category – user functionality	Data	Data retention period	Additional detail
Forensic investigations	Please refer to Data Retention and Information Management Policy – Office 365		

Category – user functionality	Data	Data retention period	Additional detail
Mailbox data	Inbox, subfolders, calendar, contacts, notes, tasks, permissions, quota (mailbox size). Deleted mailbox data	Retained until the account is deleted. Retained indefinitely until the user deletes it from the deleted items folder.	All identified material will be kept in perpetuity unless deleted by the user, after which time it will be subject to the data retention rules laid out in this document. Users may restore any email (including Instant Messenger conversation history) and calendar data they have deleted in the last 180 days using the Recover Deleted Items functionality of either Outlook or Outlook Web Application (OWA). If you purge emails from the Recover Deleted Items folder, they will no longer be visible so a forensic discovery request will need to be made

Mailbox data	Configuration comprising of email address cache, signatures, rules, junk mail settings, Outlook Web App (OWA) options	Retained until the account is deleted.	to recover mailbox items within the 180-day retention period. Note: Synchronising a blank calendar from a mobile device over the server copy is not a delete (it is a replace) and as such there is no deleted data to restore. There is no user recovery process for email / calendar / tasks / contacts data outside the period noted above (180 days).

Category – user functionality	Data	Data retention period	Additional detail
Distribution Lists (DLs)	Name	Only current membership is held, no historical membership is retained.	Until the DL is deleted by the DL owner.
	DL email address	Retained until the DL is deleted	From when the DL is deleted by the DL owner.
	DL description, type, owner, visibility, membership, exclusions and other configuration data	Retained until the DL is deleted	

Centrally managed data

Category – centrally managed data	Data	Data retention period	Additional detail
Mailbox credentials	Username	2 years from when the account is deleted	
	Primary email address	2 years from when the account is deleted	Email addresses are unique to each user and not made available for reuse at any point.
	Secondary email address	2 years from when the account is deleted	Email addresses are unique to each user and not made available for reuse at any point.
	Alternate email address (this is the nhs.uk address prior to registration)	Not available	
	Password history	The last four passwords are retained by the service	
	Account status (locked, disabled, date registered, security questions, historic quota)	Not available once the account is deleted	
	Login history comprising when logged in, client used to access service	Retained for 6 months, on a rolling basis	

Category – centrally managed data	Data	Data retention period	Additional detail
NHS Directory	Closed organisation data	Retained in the NHS Directory for 3 months after closure, or until the clean-up activities are processed.	All data deleted when an organisation is removed from the NHS Directory.
	Active organisation data	Kept indefinitely until the organisation is removed from the NHS Directory.	All data deleted when an organisation is removed from the NHS Directory.
	TANSync, CSV file upload and Push Connector	No data retained for TANSync and CSV upload submissions. However, user data added or changed through TANSync or CSV upload is processed and reflected in the Portal audit records for each account in scope.	
	All admin roles (please see the Portal LA Guide > Roles and Permissions).	Data retained until the account is deleted. Admin actions are audited for 24 months (730 days).	Self-service Local Administrator access to Portal actions that are undertaken. Local Administrators (LAs) can search the Portal audit logs of the administration portal for the organisation(s) they have LA permissions with, for example who resets a user's password or re-enables a disabled account.

Category – centrally managed data	Data	Data retention period	Additional detail
Service management data	2 Years	Retained for duration of contract	Notes
	Incident logs, problem reports change management requests, Configuration Management Database (CMDB - a database where all service management configuration items are stored), Forward Schedule of Change (FSC), Request for Change (RFC)	Problem Management Database (PMDB), known issues, capacity reports and data	From when the log is created. All problem records are retained within a database.