NHSmail: Data Retention and Information Management Policy

September 2018
Version 2

Contents

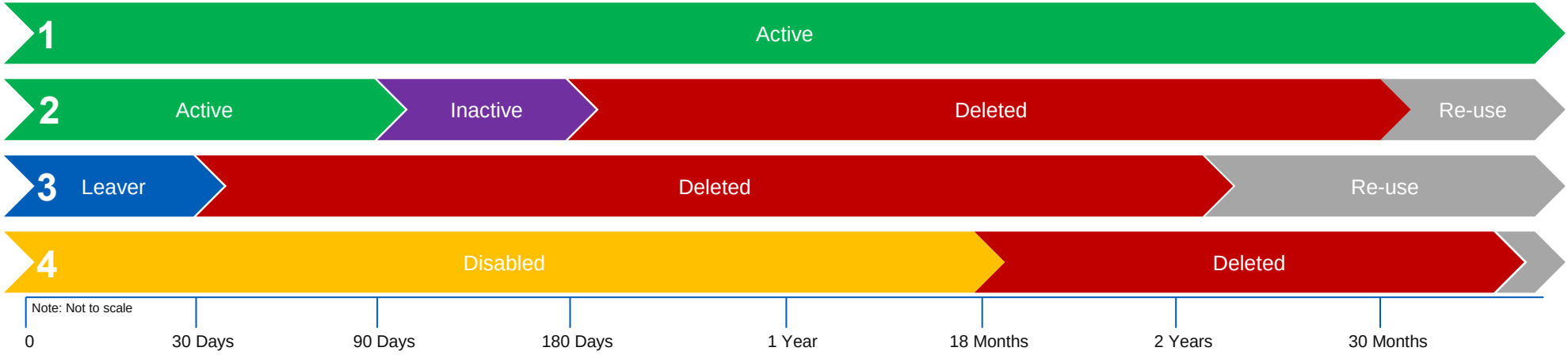
Introduction

This document defines the data retention and information management approach for the NHSmail service and defines 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 life-cycle

User accounts go through a defined life-cycle, as described below:



1. Relates to active accounts that are regularly used and have their passwords changed at least every 90-days. Active accounts will be retained indefinitely.
2. Shows the timeline for accounts that, following a password change, remain active for a 90-day period. If no action is taken, the account will become inactive for a further 90-days. After this period the account will be eligible for deletion. The account will remain deleted for up to 2 years before the email address is made available for re-use.
3. An active account that has been set as a 'leaver' by one of the organisation's Local Administrators (LAs). If the account is not joined to a new organisation within 30 days, it will be deleted. The account will remain deleted for up to 2 years before the email address is made available for re-use.
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 18-month period the account will be deleted, and any residual data securely erased. The account will remain deleted for up to 2 years before the email address only is made available for re-use.

Please note: Once an account has been removed, either via the leaver process or through inactivity, all mailbox data is securely destroyed.

Account status and retention periods

Account status	Account retention period	Additional detail
Active 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 90 days. Information on self-service password management and changing your password can be found on the Portal help pages.
Inactive person accounts (account password has expired)	Retained within the service for 6 months (180 days)	If the account password has expired after 90 days and does not have its password changed within the following 90 days (total of 180 days), it will be deleted.
Accounts marked as a 'leaver' by 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. For guidance on how to find your LA, see the guidance Finding your Local Administrator. For pharmacy, optometry and dentistry users, the LA responsibilities are carried out by the national administration service. Data relating to the current organisation should be managed in line with local information governance policies and processes. It is recommended that any data relating to the current organisation is removed by the LA and mailbox owner prior to the account being marked as a 'leaver'. The mailbox owner, prior to leaving their existing organisation, should inform their contacts that they are due to leave their current organisation and role and provide an alternate email account for all future correspondence with supporting switch over dates. For those accounts not being transferred directly or who do not immediately move into a new role and organisation, an 'out of office' message should be added to their account, informing senders they are moving organisations and telling them where to re-send their information to. Data should not be kept indefinitely in mailboxes but stored within local data repositories.

Account status	Account retention period	Additional detail
Inactive shared mailboxes	Removed after a specified period of time	Shared mailboxes that have not sent or received mail for 6 months, will be identified via communications sent to the mailbox owner and deleted after a specified period of time.
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 its status, such as re-enabling it.
Deleted accounts	Removed 6 months (180 days) after deletion.	Once an account has been deleted, it is recoverable for a further 6 months (180 days). Any requests received to recover a deleted account will be reviewed on a case by case basis.
Newly created accounts that have not been activated	3 months 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 3 months. The account name cannot be re-used for 2 years.
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.

Please note: For any account that is deleted from use, data remains available for forensic investigations as per the data retention timeframes detailed below.

Ways of accessing data

Area	Description
Audit report	To view and understand what activities have taken place by a LA or user, in the Portal. This is available by self-service in the Portal for LAs – please refer to the Portal LA Guide.
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 Policy for guidance on how to request access to NHSmail data, for the purpose of official investigations. A mailbox snapshot / dummy mailbox 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.

Please 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

Category – user functionality	Data	Data retention period	Additional detail
Forensic investigations	Full email message	6 months (180 days) Note; the default data retention period is 180 days however, the user may purchase additional data storage of 500mb increments to increase the data retention period beyond 180 days for deleted items. Information on top-up and additional services is available on the Portal help pages.	The full email message, including any email attachments, is retained for 180 days from the date it was sent (via NHSmail) or received (from an external email service). The 180-day period begins from when the supplier instigates the request. Note; this is for NHSmail only, nhs.uk to nhs.uk traffic logs are available from the sending and receiving systems. Application accounts do not have data retained for forensic auditing as this will be done by the application itself.
	Email summary	24 months (730 days)	Meta data only (to, from, subject, time / date). Note; this is for NHSmail only, nhs.uk to nhs.uk traffic logs are available from the sending and receiving systems.
	Account system logs	6 months (180 days)	Log on date / time, device name, successful / unsuccessful logon attempts.

Category – user functionality	Data	Data retention period	Additional detail
Forensic investigations (continued)	Instant Messenger conversation	6 months (180 days)	Automatically saved to the 'conversation history' mailbox folder and remains there until the user deletes it. If deleted by the user, the conversation history is available through the forensic discovery process. If file sending is enabled on a per organisation basis for Instant Messaging and Presence, then information is retained on the file name and time it was sent. **Exclusions:** screen shares, presentations in meetings, voice or video using Skype for Business. Accounts programmatically creating email messages. Application accounts do not have data retained for forensic auditing as this will be done by the application itself.

Category – user functionality	Data	Data retention period	Additional detail
Mailbox data	Inbox, subfolders, calendar, contacts, notes, tasks, permissions, quota (mailbox size).	Retained until the account is deleted.	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.
	Deleted mailbox data	Retained indefinitely until the user deletes it from the deleted items folder.	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 to recover mailbox items within the 180-day retention period. Please 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
Mailbox data (continued)	Configuration comprising of email address cache, signatures, rules, junk mail settings, OWA options	Retained until the account is deleted.	
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	24 months (730 days)	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	
	Secondary email address	2 years from when the account is deleted	
	Alternate email address (this is the nhs.uk address prior to registration)	Not available	
	Password history	The last 4 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.

NHSmail Office 365 Hybrid

NHSmail Office 365 Hybrid provides a configured central Office 365 (O365) tenant. The NHSmail Active Directory with Microsoft Azure AD synchronisation enables users to sign into NHSmail, O365 and other Azure services using their NHSmail user name and password.

Organisations can subscribe and manage their own O365 users within NHSmail via the existing NHSmail Portal, which has been enhanced to provide access to administration features for O365 services such as assigning licences, enabling applications and creating SharePoint sites.

The NHSmail Live Service, including NHSmail O365 Hybrid, is compliant with the Data Protection Act 2018. Further information is available on the Portal help pages in section “GDPR”. As a Joint Controller, local organisations must complete their own Data Protection Act 2018 compliance statements if they wish to use the NHSmail O365 Hybrid.

Any data that resides in O365, including personal data, is the responsibility of local organisations and is subject to local information governance and clinical safety practices. Local organisations must update transparency information to record how this data is captured and stored.