MI-(28331)

MAJOR INCIDENT REVIEW
(Mail Retention Policy Incident)

Service(s) Affected:
Microsoft 365 Tenant Management and Office 365 - Exchange On-line.

Document Version	1.0

Status	Approved

Document author:	Simon Medicke	
Review date:	27/03/2023	
Approved by/Date Approved:	IRLG	25/05/2023
Document Location:	Major Incident SharePoint site	

TŶ GLAN-YR-AFON 21 Cowbridge Road East, Cardiff CF

TŶ GLAN-YR-AFON 21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD

STRATEGIC OBJECTIVE	Delivering High Quality Digital Services

WELL-BEING OF FUTURE GENERATIONS ACT	A healthier Wales
If more than one standard applies, please list below:	

DHCW QUALITY STANDARDS	N/A

HEALTH CARE STANDARD	N/A
If more than one standard applies, please list below:	

IMPACT ASSESSMENT	
QUALITY AND SAFETY IMPLICATIONS/IMPACT	No, there are no specific quality and safety implications related to the activity outlined in this report.
LEGAL IMPLICATIONS/IMPACT	No, there are no specific legal implications related to the activity outlined in this report.
FINANCIAL IMPLICATION/IMPACT	No, there are no specific financial implication related to the activity outlined in this report
WORKFORCE IMPLICATION/IMPACT	No, there is no direct impact on resources as a result of the activity outlined in this report.
SOCIO ECONOMIC IMPLICATION/IMPACT	No. there are no specific socio-economic implications related to the activity outlined in this report

TABLE OF CONTENTS

1 INCIDENT SUMMARY (Link to timeline)

1.1 Overview

On February 16th, 2023, the DHCW Microsoft 365 Centre of Excellence (M365 CoE) uncovered an issue with email retention policies that were designed and implemented with support from TPXimpact *(formally RedCortex)* to ensure information within our Microsoft 365 Tenant is kept for a 7-year period.

The team uncovered an issue where mailboxes that were no longer in use *(i.e., did not have a license attached, so inactive)* were getting permanently deleted after 30 days. Therefore, this meant that mailbox data was being wiped for staff members who had left NHS Wales, and for staff members who had moved between NHS Wales Organisations where the mailbox had not transferred with them. Litigation hold *(where this was used)* protected some mailboxes from deletion. This issue did not affect live mailboxes.

This retention functionality is limited to specific Microsoft licensing. This being E3 licensing under the initial Microsoft Enterprise Agreement (EA), and all licensing types (F3/E5) under the current Microsoft EA.

This issue has affected all organisations aligned to the Microsoft 365 NHS Wales tenancy agreement i.e., all Health Boards, Trusts, Special Health Authorities, Primary Care organisations in NHS Wales who hold the required level of licencing.

1.2 Root Cause

Problem Management investigation under Problem - 28331 (cymru.nhs.uk) highlighted initial configuration of the Microsoft 365 Tenant as being the root cause. The issue had been masked due to some organizations having additional retention controls in place.

1.3 Incident Investigation & Impact to users

Incident Investigation:

This concern was first proposed as a problem by Cardiff & Vale University Health Board (CAV) on Thursday 16th February, 2023 where Problem - 28331 (cymru.nhs.uk) was created by the Identity and Collaboration Services (ICS) team to investigate.

ICS replicated live retention policies to a DEV/TEST environment and begun testing with a few users, creating, and deleting them to see if they became inactive in-line with the retention hold policy requirements. They did not become inactive and were subsequently soft deleted instead. A Microsoft Purview hold was then created and tested which resulted in the users becoming inactive.

Digital Health and Care Wales (DHCW) understood that the design from contractors TPXimpact *(formally RedCortex)* around retention hold would make disabled or deleted user mailboxes inactive rather than soft deleted and retain the email data under the retention policy for 7-years. Conclusion from this testing found this not to be the case.

A call was logged with Microsoft (Case: 35017904). Microsoft also tested and confirmed the retention hold policy problem and issued the following statement:

Correct retention policy in Exchange only retains data on active mailboxes, and as soon as the user / mailbox is no longer (past the soft deleted stage) the mail is no longer retained or recoverable after 30 days. It has always been working like this as Retention Policy works on Messaging Records Management (MRM) and doesn't apply any hold on the mailbox. Retention Policy Purview adds a hold for the time-period we have specified and moves the mailbox to inactive.

On Friday 17th February 2023 at 09:00hrs the open case with Microsoft was increased to Severity A and ICS worked with the appropriate escalation Engineers confirming the situation. A priority at this stage was to ensure that no further mailbox data would be deleted.

Once satisfied that no further mailbox data was at risk the Microsoft case was lowered to Severity B.

On Tuesday 21st February, 2023 Call - 8265726 (cymru.nhs.uk) and Call - 8265735 (cymru.nhs.uk) were logged by CAV reporting absence of inactive mailboxes. They added that this was conflicting with Microsoft Documentation and suggesting that the Retention Policy was not being applied.

With no further mailbox data at risk from deletion work now focused on a permanent solution for implementing a correct mailbox retention policy, this being 7-year retention for both active and inactive mailboxes based on a Microsoft Purview solution.

Microsoft Purview Information Protection is part of our Microsoft 365 E5 Licensing Compliance Suite and provides a unified data governance solution to help manage and govern on-premises, multi-cloud, and software as a service (SaaS) data. It provides ability to create a holistic, up-to-date map of the data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

Working with Microsoft Change - 119530 (cymru.nhs.uk) was logged on Friday 17th February 2023 and approved at CAB for implementation on Thursday 9th March 2023. This change was to follow a Microsoft recommended approach to create a Microsoft 365 Purview Retention Policy and scope that policy out to all Exchange recipients across our NHS Wales Microsoft 365 Tenant. This retention policy would be set to retain data for 7 years. A second Microsoft 365 Purview Retention Policy would also be created and scoped only to health boards that were using a 'never delete' policy. This was required to ensure the same configuration was

migrated from the existing MRM policies and to avoid any data loss for Cardiff and Vale University Health Board (CAV) during their Personal Storage Table (PST) importing project.

On Thursday 9th March 2023 implementation of the change was aborted due to a 1,000 user include/exclude limit which CAV were exceeding. Unable to implement the policies as described in the change, further work was required towards finding a better fit solution. A new change would need to be built, tested, and approved at CAB.

On Friday 10th March 2023 Change - 120190 (cymru.nhs.uk) was logged and approved at CAB for implementation on Wednesday 15th March 2023. With the attempt to implement a static style Microsoft Purview Retention Policy needing to be aborted due to the size of our NHS Wales tenant and a specific exclusion limit (1,000 users), a new approach was taken using an Adaptive Purview Retention Policy. The adaptive policies have no limits but require Adaptive Scopes to be created which are then assigned to the policy.

A successful implementation of this change took place between Wednesday 15th March and Wednesday 22nd March 2023. Adaptive Scopes were created as per the Implementation Plan. Hywel Dda University Health Board (HDD) and Cardiff and Vale University Health Board (CAV) group members were set with a custom attribute value Purview Retention Exchange Never Delete policy. Adaptive Retention Policies were then created and implemented for remaining organizations as per the implementation plan.

CAB were notified of this successful mail retention policy incident resolution and the change record was closed on Tuesday 30th March 2023. Ongoing investigations to business impact would continue under Problem - 28331 (cymru.nhs.uk).

Impact to users:

This issue did not affect live mailboxes, it impacted inactive mailboxes only.

Some organisations had implemented additional controls (a 'Hold') which provided further overriding email retention capabilities, namely: Litigation Hold and InPlace Hold. Accounts with these additional capabilities were not affected by this issue (i.e., they have not been deleted).

Following a lengthy investigation, including a survey issued to all NHS Wales organisations, a report on the current use of Litigation Hold has been produced *(see below).* In total 27,326 accounts have Litigation Hold enabled as of 24th April 2023. This constitutes approximately 17% of mail accounts.

	Litigation Hold enabled	
Organisation	TRUE	FALSE
ABMU	407	20654
Aneurin Bevan	1689	16076
BCUHB	275	29918
CAV	700	18071
CHC	99	53
Cwm Taf	351	12817
Dentists		34
DHCW	1011	774
HEIW	28	857
Hywel Dda	2167	13471
Junior Doctors	2393	2483
Leavers	151	494
National Services	3	5
NHS Wales Executive	100	159
NIA	18	13
NWSSP	156	2397
Palliative Care	14	15
Pharma	414	3112
PHW	2329	732
Powys tLHB	231	3482
Primary Care	10855	3720
Prisons	108	108
Third Parties	1	111
Transfers	208	5
UNKNOWN	6	4
Velindre CC	1429	524
WAST	1722	4424
Welsh Blood	461	230
Totals	27326	134743

The investigation also determined that two NHS Wales organisations have separate backups of mail for staff who have left those organisations, this constitutes approximately a further 30,888 accounts.

So, in total 58,214 accounts had additional backup/retention capability, this constitutes 36% of accounts. Therefore, it can be estimated that 64% of accounts did not have additional backup/retention capability and have therefore been lost.

It is not possible to report on the number of inactive mailboxes that have been deleted as there is no central identity management system in place. Every NHS organisation is responsible for managing user accounts and should have historical records for user accounts and mailboxes. It is possible to approximate the number of deleted mailboxes by referring to the number of inactive OneDrive accounts *(information which is available).* There are currently 37,812 inactive OneDrive accounts spanning the period of the last 7 years.

Therefore, the best estimate of impact is that there are approximately 38,000 users *(leavers and movers)* affected by the issue. This figure is subject to the following caveats:

1. Not all these users would have had OneDrive enabled
2. Some accounts have litigation hold in place which means retention is in place

There is no inherent Information Governance (IG) privacy risk from a Personal Information perspective as the

information has been deleted. A breach *(in Data Protection Terms)* is reportable if individual Data Subjects Rights and Freedoms are likely to be compromised. Given the current state of investigation and analysis this is unlikely and given the medium by which information is stored it's unlikely that items such as clinical information, clinical decision making, or workforce related information will be held exclusively in mailboxes now deleted.

There will be an unavailability aspect to consider, and from a law perspective this might be because of individual Data Subjects or organisations making either a subject access request *(under the framework of the UK GDPR)* or Freedom of Information Act requests.

In addition to the lawful considerations there is the aspect of Public Inquiries which are set up to investigate a specific event or topic to establish facts and lessons learned, which are captured in recommendations when they report their findings. One current example is the Covid 19 enquiry.

Organisations have been formally told to retain evidence they deem relevant to decisions made during the pandemic. This will be particularly relevant to Public Health Wales Trust as one obvious example. There should be consideration on the likelihood and impact on not being able to meet a request for information and communications that may have been retained within mailboxes now deleted. An organisation may be held to account via the Inquires Act 2005.

DHCW will work with affected organisations via the Service Management Board to assess the level of risk with regards to the Covid Inquiry, Freedom of Information Requests or similar.

2 Good Practice & Follow Up Activities

2.1 Good Practice

- M365 CoE acted quickly in identifying further at-risk mailbox data and preventing its deletion.
- Excellent levels of communication between M365 CoE, SMB, DHCW and the Health Boards was always maintained.
- A set of Frequently Asked Questions (FAQs) was developed and made available to all NHS Wales Organisations.
- M365 CAB and SMB meetings were used to update representatives from across the Health Boards and Organisations.
- Listings of inactive OneDrive accounts was made available to all NHS Wales Organisations looking to investigate impacted accounts.

2.2 Lessons Learned

- Request Microsoft to undertake a review of the all-Wales tenancy, including the 7-year data retention policy configuration.
- Explore Microsoft Purview integration for governance, protection, and compliance solutions. Workshop options into operations guided by Microsoft Engineers.
- Schedule dip-check events on inactive mailboxes to provide reassurance around 7-year data policy retention success.
- Statement preparation ahead of any public enquiry or request for information i.e., Covid 19 enquiry.

- DHCW will inform affected organisations by sharing the incident report via the M365 Service Management Board and recommend affected organisations highlight the risk to retrieving information for Subject Access Requests *(or similar)* with Information Governance teams.

2.3 Recommendations

Recommendation	Technical Area	Related ITIL Discipline	Action Type	Handler	Owner	Stakeholder(s)	Priority	Target Date	Status
Microsoft all-Wales tenancy review	Other	Incident	Engagement Request	M365 CoE	TBD	All	Medium		Choose an item.
Microsoft led Purview Workshop Training	Other	Incident	Engagement Request	M365 CoE	TBD	All	Medium		Choose an item.
Mailbox Data Retention Policy Testing	Other	Incident	Technical Action	M365 CoE	TBD	All	Medium		Choose an item.
Statement preparation ahead of any public enquiry i.e., Covid 19 Enquiry	Other	Incident	Comms	M365 CoE	TBD	All	Medium		Choose an item.
DHCW to share report with M365 SMB members.	Other	Incident	Engagement Request	M365 CoE	TBD	All	Medium		Choose an item.

3 Definitions

TERM	DEFINITION
CAB	Change Advisory Board
CAV	Cardiff & Vale University Health Board
DHCW	Digital Health and Care Wales
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
HDD	Hywel Dda University Health Board
ICS	Identity and Collaboration Services
IG	Information Governance
M365 CoE	Microsoft 365 Centre of Excellence
M365 CAB	Microsoft 365 Change Advisory Board
M365 SMB	Microsoft 365 Service Management Board
MRM	Messaging Records Management
PST	Personal Storage Table

4 TIMELINE

N/A

5 ATTACHMENTS

N/A