



Australian
National
University

Privacy Impact Assessment

Enterprise Mobility Management (EMM) –
Workspace ONE

Prepared by: Helen Duke
Information Technology Services
Helen.duke@anu.edu.au
February 2023

Contents

1.	Executive summary/introduction	3
2.	Project description.....	3
3.	Primary objectives of the EMM	5
3.1	Asset On-boarding and Inventory	5
3.2	Secure device wipe.....	5
3.3	Device encryption.....	5
3.4	Device location	5
3.5	Application provisioning.....	5
3.6	Application configuration and setting management.....	5
3.7	Enhanced security for at risk overseas travel	5
4.	Threshold assessment	5
5.	Consultation with stakeholders.....	6
6.	Information flows	6
6.1	Management methods.....	6
6.2	Data collection.....	7
	<i>What personal information is captured?</i>	7
	<i>How will the personal information be collected?</i>	8
6.3	Data management.....	8
	<i>Cybersecurity approval</i>	8
	<i>Who will have access to the personal information?</i>	9
	<i>How can individuals request access to and/or correction of their personal information?</i>	9
	<i>When will the personal information be deleted/destroyed?</i>	10
7.	Privacy management	10
8.	Conclusion/recommendations.....	12

1. Executive summary/introduction

ANU provides mobile devices to certain groups of users across the campus. ANU also supports the concept of “Bring Your Own Device” (BYOD) to allow users to utilise their personal mobile devices to access ANU information and systems. Until the implementation of the Enterprise Mobility Solution (EMM), the ANU did not have a single consistent method to manage and monitor the mobile devices used within the University. In addition, there was no standard way to manage the security of ANU owned critical data contained on these devices, and no way to maintain and manage applications running on them.

EMM is an approach to securing and enabling employee’s use of mobile devices and securing critical corporate data access and stored on these devices. EMM involves the combination of Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM). MDM focuses on locking down mobile devices, while MAM focuses on controlling which users can access which applications and MCM focuses on allowing only approved applications to access corporate data or transmit it.

In 2017, workshops were conducted with targeted groups from Colleges, Schools and business areas within the University to identify the state of management of mobile devices and the major pain points around it. The workshops helped identify business requirements for a solution that would help monitor mobile devices used across the University, increase levels of assurance and security on these devices, and improve operational efficiency and customer satisfaction.

A Request for Information (RFI) was conducted in May 2017 to gather information on available solutions and capabilities that address enterprise mobile security, availability and device management requirements. Following the RFI, a business case was approved for implementing EMM across the University and a Request for Proposal was undertaken. Following this, VMWare Workspace One was selected as the preferred tool.

The Enterprise Mobility Management project was completed in December 2019. At the time of implementation, there were approximately 575 ANU-managed devices used across the campus, mostly Apple iPhone and iPads, with some use of Android, Windows and Macintosh devices.

2. Project description

A risk assessment was conducted to understand the extent of the mobile computer platforms owned by either the University or by individuals, accessing the University’s systems and carrying University owned critical information. As a result of the findings, it was recommended that the University maintain a centralised management of mobile devices and secure data being carried on them by employing an enterprise mobility management solution.

The EMM solution was to cover the following:

- Establish and maintain a database of enrolled devices and their properties;
- Provision mobile devices, including device registration and agent activation;
- Management and control over applications available for use on the device;
- Protect and assess the integrity of enrolled devices including managing security features such as allowing remote management of the device (e.g. enforce PINs,

reset them and remote wipe devices), ensure data protection and enforcing of IT security policies;

- Optimise the functionality and security of mobile devices used within the University whilst protecting University critical information; and
- Real- time and historical visibility of enrolled devices and their activities.

Consultation was undertaken with stakeholders from across the University in order to understand the challenges posed by existing processes and practices. Some of these issues are highlighted below:

- University and personal data often co-exist on the same device. It is problematic striking a balance between strict security control of University data vs the privacy of personal data, particularly when the device is not a corporate issued asset;
- There are multiple challenges in managing the current mobile devices as assets owned by the University;
- There is a risk of leakage of sensitive University data if mistakenly sent to employee's personal contacts;
- The portability of mobile devices poses serious challenges to the security of the devices, along with critical University information on them, as they can be easily lost or stolen;
- There is currently no control over the applications that can be installed and used on mobile devices owned by the University and no way to manage and monitor the licences or the usage of the application;
- If the devices are not kept updated with current operating systems and application software versions, there is a risk to the University network when such a device is connected.

As part of addressing the problem, the University needed to:

- Protect University data, without interfering with personal data and use;
- Ensure that users have access to the mobile applications, tools and systems they need;
- Maintain compliance with University Policies and Procedures; and
- Streamline the provisioning of devices and applications.

The University sort to implement a mobile device management solution to meet the following objectives:

- Increase administrative efficiency through centralised systems;
- Increase visibility into devices owned by the University and the ability to locate devices if lost or stolen;
- Increase visibility into devices owned by the University and ensuring that applications running on them are up to date;
- Protect and assess the integrity of enrolled mobile devices and the data on them; and
- Ensure that users follow expected University guidelines for mobile usage and accessing and storing of critical University information on mobile devices.

3. Primary objectives of the EMM

3.1 Asset On-boarding and Inventory

With the University owning a significant number of mobile assets, a method to ensure we are able to update the device automatically so that it can be seamlessly managed, has been implemented. This enables maintenance of an asset register of University mobile devices.

3.2 Secure device wipe

To mitigate the risk of sensitive University data being leaked, a mechanism to ensure that lost or stolen mobile devices are wiped of any University data has been implemented.

3.3 Device encryption

To mitigate the risk of sensitive University data being leaked or tampered with, all mobile devices support full device encryption, with the requirement for end users to use a passcode to manage the device encryption.

3.4 Device location

The capability to obtain a general location of any managed mobile device is possible, with more precise tracking capable when the device is placed into lost mode, or the user opts into more detailed tracking. This feature applies to ANU-owned devices only and would be used in the event that devices are reported as lost or stolen, or a request from law enforcement authorities is received.

3.5 Application provisioning

Both self-service and automatic user and device-based deployment of business applications has been made available through the Workspace ONE Unified Endpoint Management solution.

3.6 Application configuration and setting management

Workspace ONE Unified Endpoint Management has allowed us to make customisations to enterprise issued applications to make them more appropriate for their use case within the University.

3.7 Enhanced security for at risk overseas travel

The capability to quickly apply additional security controls to managed mobile devices has been implemented, allowing for scenarios where unauthorised physical access to mobile devices is more prevalent a risk.

4. Threshold assessment

Threshold assessment conducted 7 February 2023 and threshold met because:

- Personal information is collected by the system (e.g., Name, email, user ID);
- Personal information is stored by the system;

- Personal information is used by the system;
- The collection, storage, use and/or disclosure has not previously been assessed and found compliant.

Based on the above, a PIA is required.

5. Consultation with stakeholders

Consultation was undertaken with the following areas in the preparation of this PIA:

- Privacy Office
- ITS technical officer responsible for managing the EMM
- Information Security Office
- Staff involved in the original implementation of the EMM
- Staff involved in the deployment of mobile devices in Shared Services

6. Information flows

6.1 Management methods

In practice, Workspace ONE supports BYO and ANU devices. The management methods ANU uses are UEM Managed, OS Partitioned, or Hub Registered. The UEM Managed is used for ANU devices, while OS Partitioned or Hub Registered is used for BYO.

OS Partitioned or Hub Registered limits ANU access and the information it collects on BYO devices.

Below are the major differences between the different management modes. (Please note that ANU only uses Workspace ONE for iOS, iPadOS, and Android devices. Please ignore any references to Windows or macOS.)





UEM Managed	OS Partitioned	Hub Registered Mode	App Level (MAM)
			
<p>Device is fully managed by UEM admin</p> <p>Push commands, configurations, policies and applications to the device</p> <p>Requires Intelligent Hub and MDM Profile</p>	<p>Management restricted to only business applications and business data</p> <p>No personal information can be accessed</p> <p>Enrollment starts by installing the Workspace ONE Intelligent Hub app from the store</p> <p>Requires Intelligent Hub and MDM Profile</p>	<p>Management is limited to:</p> <ul style="list-style-type: none"> • enforce policies • wipe corporate app data <p>Exception for Windows 10:</p> <ul style="list-style-type: none"> • Administrator can apply device baselines and collect device information through sensors <p>Requires Intelligent Hub</p> <ul style="list-style-type: none"> • Administrator can't push apps to the device, user must request through Hub <p>No MDM Profile</p>	<p>Management restricted to Workspace ONE SDK apps, such as:</p> <ul style="list-style-type: none"> • Workspace ONE Web • Workspace ONE Boxer • Workspace ONE Content <p>Device registration starts with the SDK-based app</p> <p>Intelligent Hub not required for Workspace ONE productivity apps:</p> <ul style="list-style-type: none"> • However, no catalog, people search, notifications, etc. <p>No MDM Profile</p>

Figure 2. Device management mode comparison

6.2 Data collection

What personal information is captured?

The following information is collected based on the device enrolled:

	ANU device	Shared ANU device	Personal device	
Location - GPS Data	collected	not collected	not collected	X
Telecom - Carrier/Country Code	collected	collected	not collected	X
Telecom - Roaming Status	collected	collected	not collected	X
Telecom - Cellular Data Usage	collected	collected	not collected	X
Telecom - Call Usage	collected	collected	not collected	X
Telecom - SMS Usage	collected	collected	not collected	X
Telecom - Device Phone Number	collected	collected	not collected	
Applications - Personal Application	collected	collected	not collected	
Applications - AirWatch SDK Application	collected	not collected	not collected	
Profiles - Unmanaged Profiles	collected	collected	not collected	X
Network - Public IP Address	collected	not collected	not collected	X
User Information - First Name	collected	collected	collected	
User Information - Last Name	collected	collected	collected	
User Information - Phone Number	collected	collected	collected	
User Information - Email Accounts	collected	collected	collected	
Device Info - Organization Group	collected	collected	collected	
Device Info - Smart Groups	collected	collected	collected	
Device Info - Phone Number	collected	collected	collected	
Device Info - Serial Number	collected	collected	collected	
Device Info - Build	collected	collected	collected	
Device Info - UDID	collected	collected	collected	
Device Info - Asset Number	collected	collected	collected	
Device Info - Power Status	collected	collected	collected	X
Device Info - Storage Capacity	collected	collected	collected	X
Device Info - Physical Memory	collected	collected	collected	
Device Info - Battery Level	collected	collected	collected	X
Device Info - Network Tethering	collected	collected	collected	X
Device Info - Time Zone	collected	collected	collected	X

For reference, here is a link to [VMWare Workspace ONE Privacy Disclosure](#). Parts I, VIII, IX, and X are applicable and are used in the current system build. This contains detailed information about what can be collected when using Workspace ONE.

How will the personal information be collected?

The data is collected when the device is first enrolled into Workspace ONE. Those items indicated (X) in the previous table will be updated, if the information has changed, when the device checks in to Workspace ONE (for detailed information on the frequency of check in, see [Updates to Check-In Intervals in Workspace ONE UEM \(2960399\) \(vmware.com\)](#)).

The GPS option does not function similarly to traditional GPS apps (real-time data collection) within Workspace ONE. Information only updates when the device moves across cell towers or Wi-Fi hotspots. Additionally, GPS information is only updated when the Intelligent Hub sends a sample of information (roughly every 500 minutes).

All of this is done only to get an approximate location of the device rather than real-time tracking.

The collection of GPS coordinates relates to privacy concerns in a fundamental way. While it is not appropriate to collect GPS data for employee-owned devices, the following notes apply to all devices enrolled in Workspace ONE UEM:

- Only the Workspace ONE Intelligent Hub relays device GPS location data back to the UEM console.
- The ANU use of GPS is for lost or stolen devices or law enforcement request. It is also used when knowing the location of a device is inherently part of the Workspace ONE UEM console function such as Geofencing.
- When GPS data is reported, Workspace ONE UEM defines a 1-kilometer region around this location. It then reports location information whenever the device moves outside the region or whenever the user opens a Workspace ONE UEM or internal application. No new GPS data is reported unless one of these actions occurs.

Note: based on privacy policies on **iOS devices**, MDM providers cannot enforce that an end-user shares location info. The end-user always has the option to turn off location access to Intelligent Hub in which case no information will be reported.

A key pre-requisite for this to work is to have the Location setting enabled on the app. The options are **Never, Ask Next Time Or When I Share, While Using the App, or Always**.

6.3 Data management

Cybersecurity approval

The requirement for an EMM was a key enabler for management of risk under the ANU Strategic Plan 2017-2021. The ANU did not have a single consistent method to manage and monitor mobile devices used within the University. In addition, there was no standard way to manage the security of ANU owned critical data that is contained on these devices, and no way to maintain and securely manage applications running on them.

A business case was approved by the IT security manager and acting Director ITS in August 2017, and the implementation of the EMM was undertaken by the Cyber and Digital Security team, which is now part of the Information Security Office (ISO). ISO continued to

manage the platform until recently (Dec 2022) when operational management was transferred to ITS.

Who will have access to the personal information?

Information stored in Workspace ONE such as device info, username, full name, email address, location, and SIM information, etc., can be accessed by the following administrative teams:

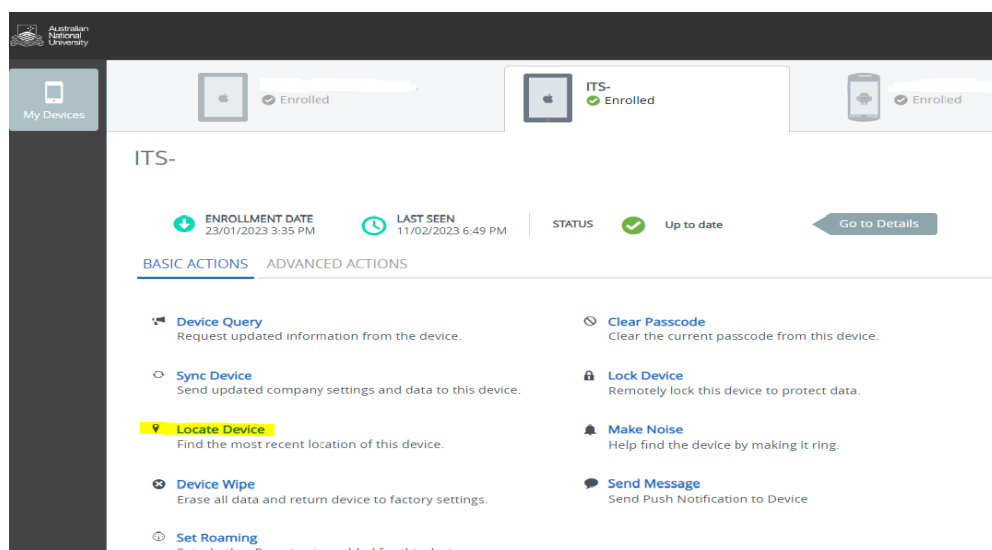
- ITS SOE Team
- ISO Server Admin
- ITS Precincts Teams
- ITS - Service Desk Level 1
- ITS – Service Desk Level 2
- UA ITS Deployment Team

The data is only used, if required, for security and device management purposes (e.g., if a device is stolen, the data will be accessed to remotely wipe the device).

Application data on the device cannot be accessed by any ITS administrators.

The user can view device and personal information through the Workspace ONE Self Service Portal (see screenshot below). The portal can be accessed via:

<https://emm.anu.edu.au/MyDevice/Landing/#/MyDevice/Device/Actions/Basic/275439>



How can individuals request access to and/or correction of their personal information?

Individuals can lodge a ticket with the ITS Service Desk requesting details and/or correction of their information, noting that the information contained in Workspace ONE is extracted from either the device (e.g., serial number) or other systems (e.g., Active Directory for name details).

The user can view their personal information through the Workspace ONE Self Service Portal (<https://emm.anu.edu.au/MyDevice/Landing/#/MyDevice/Device/Actions/Basic/275439>).

When will the personal information be deleted/destroyed?

Un-enrolling or wiping of a device removes user information associated with the device, but not device information. The device information is removed when the device is deleted from the system. This usually occurs when a device is decommissioned from service but may occur if the device is lost or stolen.

Enterprise wipe

- This is triggered when the employee leaves the organisation but they are keeping their mobile device. This applies to personal mobile devices (BYO) and ANU devices.
- If the user's manager requests it and there is a valid reason to do so. Applies to personal mobile devices.

Device wipe

- If the device is lost or stolen.
- If the user's manager requests it and there is a valid reason to do so. Applies to ANU devices.
- If the device is to be decommissioned or removed from the asset inventory.

The user does not have access to the Workspace ONE console to initiate enterprise wipe, device wipe, or device tracking. However, since the user has access to the device, they can initiate these tasks directly on their phone. For example, the user can un-enrol the device which will remove ANU data.

The user can also view their personal and device information through the Workspace ONE Self Service Portal which enables a number of functions to be completed. (<https://emm.anu.edu.au/MyDevice/Landing#/MyDevice/Device/Actions/Basic/275439>).

Note University Records is required to comply with the [Administrative Functions Disposal Authority](#) and an [ANU-specific authority for Student, Research, and Teaching and Learning files \(PDF, 3.45 MB\)](#) for records.

7. Privacy management

#	Privacy Impact	Necessity/Impact Rating/Impact Response	Impact treatment Plan
1	Personal information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Low. Information collected is for the management and monitoring of devices only.	Users are advised when the device is deployed of the purpose for which the information is collected. Authorised use is ensured through limiting access to administrative teams for the purpose of device management. Limited personal information is held in the system. All administrative staff with access have completed the Pulse Privacy course.
2	Consent for collection, use or disclosure of	Low. Staff are required to comply with policies and procedures	Acceptable use of information technology ANU Policy Library -

#	Privacy Impact	Necessity/Impact Rating/Impact Response	Impact treatment Plan
	information may not be valid.	under their employment conditions. Devices are ANU-owned or used to conduct ANU business.	Policy - Acceptable use of information technology Guidance related to use of Mobile Devices Mobile Devices - Staff Services - ANU Enterprise Mobility Management Frequently Asked Questions IT Knowledge - Enterprise Mobility Management (EMM) FAQs (anu.edu.au)
3	Individuals may be surprised or upset by a secondary use or disclosure, resulting in privacy complaints and/or negative publicity.	Medium. No personal information will be disclosed except user name, phone, email and UID. Information is only held for the purpose of device management.	There is no secondary use of the information. Access to the information is limited to administrative teams and only for the purpose specified. ANU Policy Library - Procedure - Information technology account management and access
4	The organisation or agency does not have basic information security standards in place.	Low. EMM is specifically enabled on corporate devices to improve information security.	ANU Policy Library - Standard - Infrastructure security classification
5	Individuals are not able to easily access and correct their personal information.	Low. Minimal personal information is kept.	Users are able to request information or update to data by lodging a service request ticket through the ITS Service Desk 02 61254321 or via the Service Desk Portal The user can also view their device and personal information through the Workspace ONE Self Service Portal (https://emm.anu.edu.au/MyDevice/Landing/#/MyDevice/Device/Actions/Basic/275439).
6	Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	Low. Information is obtained directly from the device or other ANU system (e.g., Active Directory).	Access to the information is limited to administrative teams and only used for the purpose specified.

8. Conclusion/recommendations

This Privacy Impact Assessment (PIA) document has been created based on the PIA guidelines set out by the OAIC (Office of the Australian Information Commissioner).

ITS will review and update this PIA document when any changes in the EMM solution make this necessary.

ITS will also work closely with the ANU privacy officer for necessary guidance around the privacy compliance requirements throughout the implementation.

ITS will ensure all staff with access to personal information through the EMM have completed the ANU Pulse module on privacy (noting this is mandatory for new staff from early 2022).

Approved



Roxanne Missingham

Privacy Officer

22 February 2023