Committee **Digital Services Sub Committee**	**Dated:** 4th November 2021
Subject: Mobile Device Management	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	**9**
Does this proposal require extra revenue and/or capital spending?	**N**
If so, how much?	**£**
What is the source of Funding?	**N/A**
Has this Funding Source been agreed with the Chamberlain's Department?	**N/A**
Report of: Chief Operating Officer	**For Decision**
Report author: Sam Collins	

Summary

This paper proposes an enhancement to the management of corporate mobile devices (Apple iPhones and Apple iPads) to introduce corporately managed Apple IDs. This would allow the City Corporation to better manage security updates, manage a corporate mobile applications list and move to a fully managed storage model utilising corporate applications such as Outlook and OneDrive, rather than device storage or personal iCloud storage. This move would also allow for the better management and tracking of these devices, including the deployment of security updates, through the corporate mobile device management tool (Intune).

Recommendation(s)

Members are asked to agree the following recommendation:

1. The IT Division moves to corporately managed Apple IDs, which would support a move towards a better managed approach for corporate mobile devices.

   And discuss

2. Members' views are sought on whether these changes should be implemented for all City Corporation device owners, or restricted to officers' devices only.

Main Report

Background

1. The City of London Corporation utilises Apple iPhones and iPads as the corporate mobile devices for both officers and Members. There are currently more than 1000 iPhones and iPads in use.

2. In January 2021 the support for Mobile devices was brought in-house and is currently provided by the Technology Support Team. Mobile Support was previously provided by Agilisys as part of the Managed IT Service Contract. In May 2021 the IT Division implemented a new provisioning model, including a self-service ordering process for officers. The intention was that mobile devices could be pre-configured by O2 and delivered directly to staff members office or home addresses.

3. In providing support for corporate mobile devices, the Technology Support Team have encountered challenges in being able to effectively support and manage the devices, principally around the current use of unmanaged Apple IDs.

Current Position

4. In setting up a new Apple Device, officers are currently required to log in with an Apple ID which leads to a more complicated set up process. This also poses a number of challenges for mobile support if a password is forgotten or a device is passed to a new member of staff without the previous owner logging out. The Technology Support Team has no means to reset the password or unlock the devices, and the only option is for officers to contact Apple directly. Where officers are unable to unlock devices, they can be rendered unusable.

5. The use of Apple IDs allows officers to backup all data to their personal iCloud. This cannot be supported by the Technology Support team and therefore the storage is not managed. There is also a risk that corporate data will be saved in personal iCloud storage.

6. Apple IDs also allow officers to download any application from the App Store regardless of whether they are work related or otherwise. This is in stark contrast to corporate Windows 10 devices, where the organisation moved to a managed desktop in 2017. At present there are a large number of non-work related mobile applications that are installed on corporate iPads, including FIFA Mobile, Pokemon Go and the IKEA mobile app.

7. In September 2021 Apple identified a ‘zero day’ threat which required all Apple devices to upgrade to the latest iOS version (14.8) to mitigate the threat. Without the use of managed Apple IDs, this required all device owners to upgrade their own devices, which has caused delays to all devices becoming compliant.

8. Under the current configuration, officers can choose not to configure their devices with the Company Portal. This means that the device is not enrolled in the organisation’s mobile device management tool (Intune), which makes the effective asset management and tracking of devices very difficult.

Proposal

9. The IT Division proposes to move to corporately managed Apple IDs, which would support a move towards a better managed approach for corporate mobile devices. This would not only simplify the set up process, but would also prevent devices from becoming blocked and allow essential security updates to be remotely deployed to devices. It would also restrict the use of personal iCloud storage and non-work related mobile applications. All devices would be automatically enrolled to the mobile device management software, making them easier to track and manage as corporate assets.

10. In implementing this new management approach, there would be two key activities required to enable the change;

    a. Device owners would be required to copy any data (photos, documents, contacts) saved on the device into one of the corporately managed mobile applications such as Outlook or OneDrive.

    b. Device owners would need to request that any existing applications are added to the approved applications list, subject to appropriate business justification. These would then be made available for download through the Company Portal. Any applications that are not corporately approved would be removed from devices once the policy change is implemented.

11. Sufficient notice (2-3 months) would be given to allow device owners to make these changes, with guidance documents made available. Where device owners are unable to make these changes themselves, the Technology Support Team would organise a series of drop in sessions where they would be available to assist.

Options

12. Members’ support is sought to take this important step in enabling a better managed mobile device estate.

13. A key decision is required on whether this policy change should be applied for all corporate Apple devices, or whether this should be restricted to officers only, with elected Members continuing with the current device management approach.

Sam Collins
Head of Change and Engagement
IT Division
E: sam.collins@cityoflondon.gov.uk
T: 020 7332 1504