worcestershire
countycouncil

CORPORATE AND COMMUNITIES OVERVIEW AND SCRUTINY PANEL 23 MAY 2022

THE COUNCIL'S IMPLEMENTATION OF MICROSOFT INTUNE (MOBILE DEVICE MANAGEMENT)

Summary

1. The Panel has requested information on the Council's implementation of Microsoft Intune (which is part of Microsoft EndPoint Manager).

2. Microsoft Intune is used by the Council to control how devices are used, including mobile phones, tablets, and laptops. It enforces a conditional access policy that ensures devices are compliant with the Government's security standards. Connectivity to council services e.g. email, OneDrive, MS Teams is no longer allowed from devices that are not verified as compliant with the Government's security standards.

3. The Cabinet Member with Responsibility for Corporate Services and Communication (CMR) and the Strategic Director of Commercial and Change have been invited to attend the meeting to respond to any questions from Panel members.

Background

4. The Council has sought to increase productivity of its workforce by enabling access to business email, calendar, and tasks from mobile devices. Whilst this was focused at corporately owned mobile devices, the previous implementation of this using Microsoft Exchange ActiveSync had resulted in any mobile device (including personal devices, subject to the use of a valid username/password) being able to connect and download Council data. Microsoft Exchange ActiveSync is a server technology not software that runs on the device in question. As such, prior to our implementation of Microsoft Intune, no software was installed on a device. This subjected the Council to several vulnerabilities as follows:

i. When a user leaves the Council, their account is disabled. However Worcestershire County Council (the Council) data on the mobile device was previously neither automatically nor manually wiped, as the only option available via Microsoft Exchange ActiveSync was the complete wipe of the mobile device resulting in the employee's personal data being destroyed as well as the corporate data. This meant that staff using personal mobiles who left had to choose to manually remove the Council's email data from the device. This almost certainly could have led to a data breach with non-Council staff having access to Council data that they shouldn't.

ii. Previously, the Council's mobile devices were, in general, not managed, for example having no mandated anti-virus/malware protection. Employees could

also choose to jailbreak[1] their mobile devices (to enable custom functionality), which is a practice that significantly increases the risk of malware. This could lead to data loss from an infected device.

5. In February, the Council underwent reaccreditation of Public Services Network (PSN) by the Government Digital Service (GDS). The position at the time was that the Council failed due to the current position on managing mobile phones; however, the pass was conditionally granted on the basis that the Council commit to implementing full conditional access of all mobile phones to corporate data by 30 April 2022. If the Council did not agree to this condition, then its PSN accreditation would be rescinded.

6. To mitigate these risks the Council implemented Microsoft EndPoint Manager (which brings together Microsoft Intune for cloud endpoint management and Microsoft Endpoint Configuration Manager for endpoints on-premises) supported by a Conditional Access Policy that enforces this for access to email from mobile devices. This will be further expanded to all services and all devices.

7. Connectivity to email is therefore no longer possible from devices that are not verified as compliant with the Government's security standards.

Mobile Device Management (MDM)

8. MDM is a proven methodology and toolset used to provide a workforce mobile productivity tools and applications while keeping corporate data secure.

9. The Council and its workforce rely on mobile devices such as smartphones, tablets and laptops for a wide assortment of tasks. However, because enterprise mobile devices access critical business data, they can threaten security if hacked, stolen or lost. So, the importance of managing mobile devices has evolved such that IT and security leaders now provision, manage and secure mobile devices within the corporate environment.

10. MDM is a solution that uses software as a component to provision mobile devices while protecting an organisation's assets, such as data. Organisations practice MDM by applying software, processes and security policies onto mobile devices and toward their use. Beyond managing device inventory and provisioning, MDM solutions protect the device's applications, data and content.

11. Microsoft EndPoint Manager, which includes Microsoft Intune, is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). It is used by the Council to control how devices are used, including mobile phones, tablets, and laptops. On personal devices, Microsoft Intune helps make sure the Council's data stays protected and can isolate council data from personal data.

Public Sector Network Compliance (PSN)

12. PSN compliance requires the Council to meet strict security standards when processing certain types of government data and accessing government systems. It is regularly audited, and the Council must annually report its security arrangements to the Cabinet Office. It is how the Council demonstrates that its security arrangement, policies

[1] To "jailbreak" means to allow an Apple phone's owner to gain full access to the root of the operating system and access all the features. Like jailbreaking, "rooting" is the term for the process of removing the limitations on a mobile or tablet running the Android operating system.

and controls are sufficiently rigorous for it to interact with the PSN and all those connected to it. It is good practice to apply the controls and methodologies to the whole Council and not just to services that utilise PSN associated systems or information. Penalties for non-compliance are that the Council would be restricted from accessing certain government systems and information.

13. Compliance with all the above standards assists the Council in keeping up to date with its security and cyber security policies and controls. This in turn ensures that Council systems and information are kept as secure as possible against emerging threats.

14. The PSN uses a walled garden[2] approach, which enables access to Internet content and shared services to be controlled. This is because the security of any one user connected to the PSN affects both the security of all other users and the network itself. The PSN compliance process exists to provide the PSN community with:

a. confidence that the services they use over the network will work without problems
b. assurance that their data is protected in accordance with suppliers' commitments
c. the promise that if things do go wrong, they can be quickly put right.

15. The direct implications of the Council not being accredited for PSN are:
    a. Access to CIS Searchlight[3] can only be obtained over the PSN network. CIS Searchlight is needed as part of the Blue Badge Service application process.
    b. Without Conditional Access and without PSN Accreditation the Council would NOT be able to connect the HSCN, as we would be unable to meet the requirements. This would prevent access to:
        - Integrated Care Record[4]
        - Carenotes[5]
        - EVIE[6]
        - Collaborate sharing with the NHS.
        - Prevent NHS obtaining access to Liquidlogic[7].
    c. Worcestershire Children First rely on PSN Accreditation to enable access to data controlled by Department for Education e.g. benefits.
    a. Access to the Health and Social Care Network (HSCN)[8] is dramatically made easier by having PSN Accreditation as it results in a significant number of questions not having to be answered.
    b. The Council relies on PSN Accreditation to support bids for funding/paid work.

[2] A walled garden is an software system wherein the service provider has control over applications, content, and/or media, and restricts convenient access to non-approved applicants or content.

[3] The Customer Information System (CIS) is used by the Department for Work and Pensions (DWP) to store information such as name, address, date of birth, National Insurance number.

[4] An Integrated Care Record (ICR) is a way of bringing together the various electronic records of a person's care. It takes information directly from existing systems used by health and social care organisations and presents it in a structured, easy-to-read format for health and care professionals.

[5] Carenotes is web-based child health, community & mental health system.

[6] Electronic View for Interoperable Exchange

[7] Liquidlogic's social care software

[8] The Health and Social Care Network (HSCN) is a data network for health and care organisations which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently while benefiting from improved network and bandwidth capacity, financial savings and easier and smoother access to clinical systems.

Cyber Security

16. Throughout 2020 and into 2021, there was a significant and concerning increase in cyber-attacks, including ransomware attacks, on the public sector and education organisations. Ransomware is often used by cyber criminals in a way that doesn't initially target specific organisations. Once the malicious software is on a network, the criminals can monitor and control the encryption of data. Their aim is to encrypt, steal or leak data that will have the biggest impact on the organisation's services. The data held by these services is also at significant risk, including personal information (the electoral register), financial transactions (revenue and benefit payments), vulnerable people (adult social care), and school data (admissions, at risk children).

17. The Council has already invested in a range of measures to protect ~~our~~ systems and the data they hold from potential attacks. These include:

a. Implementing modern firewalls and scanning services.
b. Implementing infrastructure solutions to improve the resilience of services if, and when, a cyber-attack occurs.
c. Introducing training for the workforce and elected members.
d. Maintaining compliance with the PSN[9], PCI DSS[10], and DSPT[11] security standards, to retain secure inter-working and data sharing with public sector organisations.
e. Applying the government's cyber security guidance, 10 Steps to Cyber Security[12] and Cyber Essentials[13].
f. Carrying out ongoing health checks, penetration tests and cyber resilience exercises to test our systems and processes, e.g., Web Check[14].
g. Implemented Microsoft Office Protected View that opens Office documents in read-only mode with macros and other content disabled to reduce the risk of malware and other threats.
h. Working with partners across the public sector through participation in Cyber Security Information Sharing Partnerships[15], Warning, Advice and Reporting Points[16] and Local Resilience Forums[17] to protect our systems from, and put in place plans to respond to, cyber-attacks.

18. The priority is to ensure that the Council continues to be secure and resilient to cyber threats.

---

[9] Public Sector Network (PSN) (www.gov.uk/government/groups/public-services-network)

[10] Payment Card industry data Security Standards (PCI-DSS) PCI Security Standards Council Site

[11] Data Security and Protection Toolkit (DSPT) https://www.dsptoolkit.nhs.uk/

[12] 10 Steps to Cyber Security (10 steps to cyber security - NCSC.GOV.UK)

[13] Cyber Essentials (www.cyberessentials.ncsc.gov.uk)

[14] Web Check NCSC Web Check - NCSC.GOV.UK – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils.

[15] Cyber Security Information Sharing Partnerships (CiSP) (www.ncsc.gov.uk/cisp),

[16] Warning, Advice and Reporting Points (WARPs) (www.ncsc.gov.uk/articles/what-warp)

[17] Local Resilience Forum (LRFs) (Local resilience forums: contact details - GOV.UK (www.gov.uk)

Data Security and Protection Toolkit (DSPT)

19. The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. This self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, in particular health and social care personal records.

20. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

21. The criterion relating to Mobile Device Management in the 2021-2022 DSPT is:

If staff, directors, trustees and volunteers use their own devices (e.g., phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g., if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, then tick and write "Not applicable" in the comments box. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices/)

22. The relevant BYOD[18] policy in the Council is the Communication and Mobile Devices Policy, and Microsoft Intune is the solution that the Council is using to enforce this.

The Council's Communication and Mobile Devices Policy

23. The purpose of the Communication and Mobile Devices Policy is to advise acceptable use with regard to mobile devices (including mobile phones) and communication systems used for business activities. With the convergence of data and voice and video communication systems, the ability to connect remotely to internal systems and the wide range of options offered by mobile devices, it is essential that these technologies be used by authorised persons for legitimate business activities.

24. Appendix 1 provides further information on the relevant clauses from the Communication and Mobile Devices Policy.

Benefits of Microsoft Intune

25. Secure solution for BYOD: Microsoft Intune provides a secure solution for BYOD as it ensures that the employee's device is appropriately configured to meet the

[18] Bring your own device (BYOD) refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

Government's requirements to access corporate data. It provides this assurance by automatically assessing the configuration of the device against compliance policies without having any access to any data on the device.

26. Cost: Microsoft Intune is part of Microsoft Endpoint Manager, which is bundled with Microsoft 365. The Council has already invested in Microsoft 365 licenses and is therefore paying for Microsoft Intune. There are no additional licensing costs associated with the Council's use of Microsoft Intune.

27. Central management: Microsoft Intune can be used to provision, secure, manage and monitor all the Council's endpoints centrally in one system. This will accelerate the adoption of Zero Trust[19] and facilitate better security.

28. Increased productivity: With Microsoft Intune the time taken to provision new devices can be reduced, moving to greater automation in processes.

29. Improved cyber security: All endpoints can be secured, managed and monitored from a single system – Microsoft Intune. This will enable a consistent set of security policies, device management practices and compliance rules across all devices.

30. Improved Privacy for BYOD: Mobile security threats are rising and securing data on personal devices is paramount to good security and using devices for sensitive business such as banking makes security even more essential. Without security for personal smartphones, the Council is at risk of a breach.

31. Adherence to government requirements:
    a. Encryption: Checking data stored on the device is encrypted.
    b. Patching: Checking that the device and the version of operating system is still supported by the vendor and security updates are automatically applied.
    c. Authentication: Checking that the device meets minimum username / password requirements e.g. biometrics or PIN[20] or password complexity etc.
    d. Firewall: Checking the device has a working firewall if applicable.
    e. Anti-Virus / Anti-Malware: Checking that the device is protected from viruses and malware as applicable.
    f. Secured: Checking that the device hasn't been "jailbroken" thus ensuring that only trusted code can be executed on the device via applications installed via the official Google Play / Apple App Store.

Impact of Microsoft Intune on the owners of BYOD

32. If councillors and staff want to use their personal device to access council services, then they must ensure the device is enrolled in Microsoft Intune and meets the Council's compliance requirements. Connectivity to council services e.g. email, OneDrive, MS Teams is no longer allowed from devices that are not verified as compliant with the Government's security standards.

[19] Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

[20] A personal identification number (PIN), or sometimes redundantly a PIN number or PIN code, is a numeric (sometimes alpha-numeric) passcode used in the process of authenticating a user accessing a system. In mobile devices, the PIN acts like a password preventing other people from gaining unauthorized access to the device. This is a numeric code which must be entered each time the device is started (unless the PIN security feature is turned off).

33. Failure to meet the Government's security requirements will automatically result in access to council services on personal devices being blocked.

34. By enrolling their mobile device into Microsoft Intune, IT will be able to take the following actions on their phone or tablet to make sure council information is secure. These actions would only be undertaken following consultation with the device owner.

a. Reset the phone to factory settings if it is lost or stolen.
b. Remove company-related files and apps (without removing personal files or apps).
c. Require the use of a password or PIN.
d. Remotely reset the PIN or lock the phone or tablet if it is lost or stolen.
e. Make the phone or tablet compatible with the Council's security standards, which helps the individual as well as the company.

35. Once the device is enrolled, IT will be able to see this type of information on the phone or tablet:

- Owner
- Model
- Device name
- Operating system
- Serial number
- Council apps
- Manufacturer

36. IT will not be able to see this type of information on the phone or tablet:

- Call history
- Location
- Text messages
- Camera roll
- Personal email
- Contacts and calendar
- Personal data
- Web history
- Personal apps

Impact of resetting a device to factory settings

37. IT and Digital will only reset devices to factory settings if required by the owner of the device, and in the eventuality that the device is lost or stolen. It should be noted that there are no risks of damage to the device associated with factory resetting a smartphone.

38. Factory reset also known as master reset, hard reset or hardware reset is a built-in feature for electronic devices. A factory reset erases all data, settings and applications stored on the device. It returns the smartphone to the condition it was when it was brand new.

39. Irrespective of any enrolment with Microsoft Intune, device owners can perform a factory reset themselves on their device. In addition, they can restore and recover their backed-up data after a factory reset. Most services have some form of cloud backup, for example via a Google account for Android, or iCloud for Apple users. It should be noted that there are benefits that may be achieved from a factory reset of an Android or iPhone:

i. Improves Smartphone Performance: The longer smartphones are used, the more unnecessary data it accumulates. There is also the leftover data from uninstalling apps. This data consumes a lot of storage and memory in the background and tends to slow the device down. By factory resetting, the accumulated clutter is removed. The smartphone then becomes responsive and fast as when it was brand new and is potentially a way to improve smartphone's system performance.

ii. Factory reset serves as a last resort method in solving certain serious smartphone problems. It might be that the device is stuck at starting or a malicious is causing phones issues (crashes, freezing, poor performance etc.). These problems can make it difficult to use the phone or access it at all. By resetting it to factory settings it is possible to get rid of the problem.

Impact of resetting a Personal Identification Number (PIN) on a BYOD

40. There are no risks to personal devices associated with the reset of a PIN.

41. PINs would not be reset by the Council unless specifically requested by the owner of the BYOD.

42. If the owner of a BYOD had forgotten their pin / passcode, then the Council could be contacted to reset their PIN so they could access their device again.

43. In the extremely unlikely scenario that a PIN had accidently been reset without the authorisation of the owner of the device, then the Council could be contacted to reset the PIN again so the owner could access the device.

Mobile management solutions from multiple organisations

44. In a scenario where the MDM solution from another organisation has caused a technical issue with the Council's use of Microsoft Intune on a BYOD, then the IT department would liaise with the device owner and potentially the other organisation to try to resolve any technical issue.

45. If the other organisation is using Microsoft Intune (which is becoming increasingly likely due to the costs of Microsoft Intune being part of the Microsoft 365 E3 license), Microsoft potentially provide a resolution to this as per the article below. Whilst, this functionality is still in preview, it should enable the Council to trust the MDM solution of the other organisation thus enabling scenarios where devices managed by a district council, for example, can be trusted to connect to the County Council's services.

Cross-tenant access overview - Azure AD | Microsoft Docs

Financial implication to the Council

46. Microsoft Intune is part of Microsoft Endpoint Manager, which is bundled with the Council's Microsoft 365 licences. The Council has already invested in Microsoft 365 licenses and is therefore already paying for Microsoft Intune.

47. If councillors and staff choose to access council services from a personal device, they will be required to voluntarily enrol into Microsoft Intune and meet the Council's compliance requirements before access to council services are granted. There is no financial implication to the council in this scenario.

48. The Council can provide a corporate smartphone to officers and Councillors, which will be enrolled in Microsoft Intune to ensure it meets compliance requirements. The standard smartphone currently issued is the Samsung Galaxy A13, at a cost of £139 per handset plus the monthly contract.

Communications to staff and Members

49. The implementation of Microsoft Intune has been communicated to staff and councillors. Information has been provided on the Council's intranet (OurSpace) and several emails have been issued, as well as information within the Microsoft Intune guidance documentation. The communications explain the purpose of Microsoft Intune, what the software enables IT to do on personal devices, and what information is and isn't accessible.

50. Self-service instructions on how to enrol into Microsoft Intune have been provided.

51. During the enrolment process information is provided to explain what information the Council will be able to see, what can't be seen, as well as the actions that the Council will be able to perform on the BYOD.

Options available to staff and councillors

52. The use of personal devices is absolutely an individual decision for each member of staff and councillors to make themselves, and the Council does not mandate that they do so.

53. Therefore, if councillors and staff wish to access council services from a mobile device, they have the following choice:

i. Via a Personal device: Personal devices will need to be voluntarily enrolled into Microsoft Intune and meet the Council's compliance requirements before access to council services are granted.
ii. Via a Council device: The Council will provide a corporate smartphone, which will be enrolled in Microsoft Intune to ensure it meets compliance requirements.

Purpose of the Meeting

54. The Panel is asked to consider the information provided and:

- determine any comments to make to the Cabinet Member with Responsibility for Corporate Services and Communication

- agree whether any further Scrutiny is required at this stage.

Supporting Information

- Appendix 1: Communication and Mobile Devices

Contact Points

Andrew Spice, Strategic Director of Commercial and Change
Telephone: 01905 846678
Email: aspice@worcestershire.gov.uk

Sandra Taylor, Assistant Director for IT and Digital
Telephone: 01905 845447
Email: staylor12@worcestershire.gov.uk

Emma James / Jo Weston, Overview and Scrutiny Officers
Telephone: 01905 844964
Email: scrutiny@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer, in this case the Assistant Director for Legal and Governance there are no background papers relating to the subject matter of this report:

All agendas and minutes are available on the Council's website here.

worcestershire
countycouncil

Appendix 1: Communication and Mobile Devices

The Communication and Mobile Devices (User Policy) provides the following guidance for users:

6.3	**Bring Your Own Device**
6.3.1	Personally owned communication devices may not be connected to or synchronised with the Council's computer systems or networks unless approved by the Assistant Director for IT and Digital and the device owner agrees to the security requirements regarding the management of the device. BYOD security requirements include: • Agreement that the device will be managed by the Council • Agreement for the Council security profile to be applied to the device **Explanation** the Council must be able to protect its IT resources and in order to do this it must be able to apply specific security settings and limit the functionality of the device. One of the biggest threats to corporate IT security is the portable device which is periodically connected to the corporate network as this may potentially introduce viruses and other malware and aid information leakage. Portable devices owned personally by staff or contractors may not always have the tightest security as this often impacts on functionality, e.g., password or pin protection. The Council must be able to ensure that every device connected to the computer system and/or network has the same configuration and security settings applied and therefore the level of risk is mitigated.
6.3.2	The Council corporate data and the management application must be removed and the user may be required to bring their device in for this to be achieved. **Explanation** As potentially confidential information could be stored on the device (e.g. email) the Council must ensure it is protected to the level of its sensitivity. This requirement relates to devices supplied by the Council or to a personally owned device supplied by a user. Security settings may include: • PIN or Password Protection • Autolock • Anti Virus installed where available • Personal firewall installed where available • Encryption turned on • Certificates installed • Disabling non-essential communications functionality • Limiting applications to those required for business purposes (e.g. disable Apps Store, Camera, iTunes, Cloud Storage Services, YouTube etc) • The ability to remote wipe the device
6.3.3	Maintenance responsibilities for mobile devices used for business purposes are as follows: • the Council owned and supplied devices will be fully maintained by the Council

	• Personally owned devices will be managed by the Council but maintained by the user Any issues must be logged with myIT Support. **Explanation** This requirement clearly defines who is responsible for devices and their maintenance. the Council will not be responsible for damage to, or loss of information incurring on personally owned devices under any circumstances. Maintenance means keeping the operating system up to date and ensuring that the device remains operational. With the development of malware designed specifically to infect mobile devices it is essential that these devices have the latest versions of operating systems installed and other protection mechanisms such as anti-virus and a personal firewall if available. Just like any other virus infection, infected devices will spread the virus to other devices and could potentially affect the computing environment itself if a direct connection can be made between the device and the internal computer network.

The Communication and Mobile Devices (Technical Policy) provides the following technical guidance:

Mobile Device Management

6.2.1	A risk assessment must be carried out by the Assistant Director for IT and Digital to confirm that mobile devices and communications systems do not create additional security vulnerabilities which are unacceptable to the Council. Managers may only approve devices that have been evaluated and approved as risk free by the Assistant Director for IT and Digital. **Explanation** The Assistant Director for IT and Digital must be satisfied that the increased automation and functionality offered by the introduction of mobile devices and communications systems is warranted when compared with the additional security threats that they introduce into the computing environment. He or she must also ensure that any device offered to a staff member is configured with the appropriate security settings and that the threat of information leakage or interception is minimised.
6.2.2	Mobile devices connecting or synchronising to the Council's computing resources must be configured with the Council security profile which may include: • Passwords or Pin numbers • Autolock • Remote Wipe • Disabling applications or functions that are not required for business purposes • Encryption and digital certificates where information is considered sensitive or confidential • Sandboxing or a no data at rest configuration • Anti Virus • Firewall

	• Device identification • Auto update of the operating system for patches and system upgrades In a BYOD situation, the user must agree to have the device managed by the Council who will ensure that it is patched and can be wiped if lost or stolen. **Explanation** Although many users will not consider a tablet or mobile phone to be a security threat to the Council, the ability to access email, customer address lists and other corporate information remotely does create security vulnerabilities if devices are not configured with the appropriate security settings. The security profile must be enforced on devices that are to be connected to the corporate network. Users are not permitted to change these settings.