

Bring Your Own Device Acceptable Use Policy

Released On	
Author(s)	Irene Docherty
Reviewed By	
Version and Date	v 1.3, 08/01/14
Master Document Index Number	IS-WC-POL-0001
Protective Marking	unclassified

1. Document Control

1.1. Distribution List

Name	Role	Signature	Date	RACI
Andy Spurway	Head of Service Delivery, Information Services			R
Tim Way and Debbie Mason-Smith	Information Security Architects, Corporate Governance			A
Mike Potter	Information Assurance and Policy Officer			R/C
Keir Eaton	Information Security Officer, Programme Office			C
Information Services Managers				C
Ian Baker	Head of Corporate Programme			C
Information Assurance Steering Group				C
Mark Stone	Programme Director Transformation			C
Margaret Roots and Amanda George	HR Policy Officer and HR Policy and Reward Manager			C
Richard Woods	Insurance Officer			C

1.2. Audit History

Version	Date	Name	Notes
1.0	21/10/13	Irene Docherty	Document created
1.1	19/11/13	Irene Docherty	Amendments after contributions from: BB, TW, PB, IB, AW, AS
1.2	06/12/13	Irene Docherty	Incorporated comments from IASG and HR (MR)
1.3	08/01/14	Irene Docherty	Incorporated comments from RW and BB

1.3. Document References

Document Name	Author	Date & Version
Technical Standard, Common Standard for Malware Protection, Public Services Network Programme	PSN Infrastructure Security and Cyber Defence Team	6 th December 2012, v. 1.0
http://en.wikipedia.org/wiki/Bring_your_own_device		[accessed 21/10/13]
Casey, Kevin (19 November 2012). " Risks Your BYOD Policy Must Address ", <i>InformationWeek</i> . Retrieved 19 June 2013.		[accessed 21/10/13]
Wiech, Dean. " The Benefits And Risks Of BYOD ". <i>Manufacturing Business Technology</i> . Retrieved 28 January 2013.		[accessed 21/10/13]
http://cxounplugged.com/2013/01/byod-policy/		[accessed 21/10/13]
Wiltshire Council Information Assurance Acceptable Usage Policy for email, internet and computer use	Information Assurance	26/02/13
ICO Bring Your Own Device Guidance www.ico.org.uk/.../ico_bring_your_own_device_by_od_guidance.pdf	ICO	[accessed 17/10/13]
Wiltshire Council Flexible Working Policy and Procedures [Accessible from HR Direct: http://thewire.wiltshire.council/hrdirect/flexibleworkingandhomeworking/flexibleworking/flexibleworkingpolicyprocedure.htm accessed 17/10/13]	Human Resources Strategy and Policy Team	Revision April 2013
<u>Information Security Management Principles</u> ISBN 978-1-78017-175-3	Andy Taylor, David Alexander, Amanda Finch and David Sutton	Second Edition, 2013
Existing mobile device management monitoring and reporting processes	Barney Brooks and Hannah Smith	Revision 22/10/13

2. Introduction

Wiltshire Council is committed to flexible working and has a suite of flexible working policies and associated guidance and toolkits. Further, Wiltshire Council recognises that Device owners wish to use their own mobile devices to access Wiltshire Council data and use Wiltshire Council applications as part of flexible working arrangements. This policy outlines the responsibilities of both the device owner and Wiltshire Council.

This document provides standards and guidance for acceptable behaviour for the use of personal devices, such as smart phones and tablets, by Wiltshire Council device owners to access network resources, namely their Wiltshire Council e-mail, calendar and Lync, for business purposes. This policy will be updated regularly to accurately reflect devices and IT Services coverage.

Access to and continued use of network services is granted on the condition that each device owner reads, signs, respects and follows Wiltshire Council's policies concerning use of these devices and services. The use of a personally-owned device in connection with Wiltshire Council business is a privilege granted to device owners through approval of Information Services management. Wiltshire Council reserves the right to revoke these privileges in the event that device owners do not abide by the policies and procedures set forth in this document.

3. What is Bring Your Own Device?

“Bring Your Own Device” (BYOD) refers to organisations permitting their device owners to bring personally owned mobile devices (e.g. tablets and smart phones) to their workplace, and use those devices to access privileged organisational information and applications.

4. Who does it apply to?

This policy applies to employees, elected members, Co-opted members, contractors and third parties who wish to connect to any of Wiltshire Council's computer systems to access Wiltshire Council's electronic data using a personal device. Third parties would additionally be required to sign an appropriate data sharing agreement or contract. At this stage there is no policy framework for allowing volunteers access to BYOD, therefore they are excluded from this policy.

You must read, understand and formally accept this policy by signing and returning the Bring Your Own Device Application Form and Acceptable Use Statement found in Appendix 2 before you can use Wiltshire Council's computer systems and equipment.

You may be asked to re-confirm acceptance annually with updates being sent out throughout the year.

5. Which Devices are Covered?

Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements:

- Android 4 or higher Smart Phones and Tablets*
- iOS 5 or higher iPhones and iPads
- Windows Mobile 8 or higher

Devices below these specifications will not comply with our policies and therefore will not be supported.

Devices that have taken part in the BYOD pilot will be covered retrospectively by this policy by completing and returning the Bring Your Own Device Application Form and Acceptable Use Statement in Appendix 2.

* Android Device owners are required to have anti-malware software installed on their devices, otherwise Wiltshire Council will deploy anti-malware software onto all Android devices under this policy. For further guidance on this, please contact the IS Service Desk on 01225 718718.

6. What IT Services are Available?

Device, Application or Data Access Limitations

The IT Services covered by policy are:

- E-mail – business e-mails are accessed and three days' worth are downloaded to the device, after which they are overwritten
- Calendar
- Contacts
- Tasks
- Lync

These are subject to normal performance management constraints.

7. Who Manages this Facility?

Information Services in conjunction with Corporate Governance will manage the BYOD facility, as described within this document, on behalf of Wiltshire Council. Human Resources will advise managers, if corporate policies have not been followed. In specific the BYOD facility includes the approval, monitoring, reporting and security incident processes, e.g. wiping the device, for all devices.

8. What Support will Information Services Provide?

Wiltshire Council will not support or maintain any personal mobile device. Further, Wiltshire Council will not cover any damage to the device. Refer to section 18 Wiltshire Council Release of Liability and Disclaimer Statement for further details. It is recommended that device owners insure their device as part of their home contents insurance and advise their insurer that the device will be used for work purposes at home and at work locations.

Upon approval of the application and installation of the mobile device management software, the device owner can connect to the Wiltshire Council infrastructure to access their Wiltshire Council e-mail, calendar and Lync at his own risk. However, the device owner is personally liable for the device and carrier service costs. They will not be reimbursed by Wiltshire Council for the acquisition of a mobile device, its use, maintenance or replacement or any carrier service charges incurred. The device owner must agree to all terms and conditions in this policy to be allowed access to the Wiltshire Council services listed in this document.

Device owners with devices that are not in line with our standard approved device lists may not be allowed to have their devices added to the servers. Owners of personal devices are not permitted to connect to Wiltshire Council infrastructure without documented consent from Information Services. Furthermore, Wiltshire Council and Information Services specifically reserve the right to disable or disconnect some or all services without prior notification.

9. Regulations and Policies

There are a number of Wiltshire Council policies and UK Primary legislation that are aimed to protect the integrity of Wiltshire Council data and ensure it remains safe and secure under Wiltshire Council control; these can be found in Appendix 1. The lists in Appendix 1 are not exhaustive and will be updated, as new policies and regulations emerge.

10. Device Owner Responsibilities

As the device owner, you carry specific responsibilities, as listed below:

- You will not lend anyone your device to access Wiltshire Council information or use Wiltshire Council infrastructure.
- Should you decide to sell, recycle, give or change your device, you will inform the IS Service Desk by phone on 01225 718718 right away or through the IS Portal.
- The policy will require a four digit pin to access your device. Your device or application will lock every 5 minutes requiring re-entry of your pin.
- In order to access your Outlook e-mail, calendar and Lync, you will need to enter your network account password. This rotates every 90 days, as per domain policy.
- Backing up your personal files and in the case of a device shared with family or friends, their personal files to your own personal laptop.
- All external email transfers of sensitive information must be a password protected zip file for RESTRICTED. If this cannot be done, then you should not be sending the information on that device.
- You must conform strictly to the council's Protective Marking Procedures for the movement of large files and information; see the Protective Marking Procedures for more information <http://thewire.wiltshire.council/index/dce-homepage/law-and-governance/ict-security-information-guides.htm>.
- You must ensure that your device is compliant and that security software is kept up-to-date. The system will check whether your device meets compliance criteria and if not, will automatically stop syncing.
- You must not use your device to store corporate e-mails, files and data.
- Your device will be automatically wiped without notice if: (i) you lose the device; (ii) you terminate employment with Wiltshire Council or (iii) Information Services detects a data or policy breach or virus; refer to sections 12-14, 16-18.
- You are responsible for the safekeeping of your own personal data.
- In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jailbreaking" your iPhone or "rooting" your android device.

Be aware that Jailbroken or Rooted devices will not be permitted as it violates the device compliance policy. Any devices that become rooted or jail broken will automatically stop syncing and will be reported to the IS Service Desk and Information Assurance teams.

11. Wiltshire Council's Responsibilities

As the data controller, Wiltshire Council is responsible for ensuring that all processing for personal data which is under his control remains in compliance with the Data Protection Act 1998.

Wiltshire Council must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect council owned data must remain proportionate to the risks. A risk-based decision will look at both the risks and opportunities as part of the decision process.

The following will need to be assessed by Wiltshire Council:

- what type of data is held;
- where data may be stored;
- how it is transferred;
- potential for data leakage;
- blurring of personal and business use;
- the device's security capacities;
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device.

12. Security Incidents

A number of security incidents could occur when using personal devices with Wiltshire Council data. These include:

- theft or loss of data or any equipment;
- transfer/disclosure of sensitive data to those who are not entitled to receive it;
- compromised passwords;
- attempt (either failed or successful) to gain unauthorised access to data or systems;
- connection of equipment that has either not been approved by Wiltshire Council;
- non-compliance with Wiltshire information security policies and associated procedures including this policy;
- hacking attempts, virus attacks, phishing etc;
- device "jailbreaking," "rooting," or the equivalent
- making any other modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator.

Performing such actions or making such unauthorised modifications is essentially an "inside attack" on device, application, and data security, and should be treated very seriously.

13. If a Security Incident should Occur

If a security incident should occur, e.g. your device is lost or stolen or is infected with malware, you are required to inform the IS Service Desk immediately with details.

Information Services reserves the right to wipe either Wiltshire Council data and applications or the whole device, if it is deemed necessary. This may impact other applications and data, such as the native Address Book data and any personal files on your device.

Generally, the following guidelines apply:

In the case of an Android device, the whole device will be wiped.

In the case of an iOS device, corporate data and applications will be wiped.

14. If You Leave the Employment of Wiltshire Council

As part of the leaver's process, your access to Wiltshire Council infrastructure and applications will cease and your device will be de-provisioned and ensure access to Council data is ceased and Council data is wiped.

15. What is the Procedure for Accessing this Facility?

Approval Process

The device owner and user will raise a Service Request through the IS Service Desk by phoning 01225 718718.

The IS Service Desk technician will e-mail the device owner a copy of BYOD policy statement to read, sign and date.

The signed form, Appendix 2, at the end of the policy document must be scanned and an electronic copy e-mailed to the IS Service Desk.

Upon receipt of the signed policy statement, the IS Service Desk will make an appointment with you to enable the mobile device management software on your device and in the case of Android devices to install anti-virus software on your device.

From the date of receipt of your signed policy statement, the anticipated time for this activity is approximately one work week.

16. Consequences for Misuse/Disruption

Breach of this policy by a Wiltshire Council employee may lead to disciplinary action, which could result in dismissal, suspension or termination of your access to the Service and/or prosecution and/or Wiltshire Council co-operating with law enforcement organisations, government agencies, other legal authorities or third parties involved in the investigation of any suspected or alleged criminal or civil offence. Please refer to the disciplinary policy and procedure for more information.

A complaint made against a councillor under this policy should be referred to the Monitoring Officer who will advise on the appropriate action to take.

17. Guidelines for Acceptable Behaviour

Device owners are expected to behave in accordance with Wiltshire Council's behaviours framework at all times whilst undertaking work for the Council. Further information can be found on HR Direct, from your manager or by contacting an HR advisor.

Be aware that any personal device used at work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against Wiltshire Council. Your data could be examined not only by Wiltshire Council but also by other parties in any lawsuit.

A further consideration is that if you travel internationally your device might be subject to search and seizure at border control.

18. Wiltshire Council Release of Liability and Disclaimer Statement

Wiltshire Council hereby acknowledges that the use of a personal device in connection with Wiltshire Council business carries specific risks for which you, as the device owner and user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

Wiltshire Council hereby disclaims liability for the loss of any such data and/or for service interruptions. Wiltshire Council expressly reserves the right to wipe the device management application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining Wiltshire Council infrastructure and services.

Wiltshire Council also disclaims liability for device owner injuries such as repetitive stress injuries developed. Wiltshire Council provides IT equipment that is suitable for long-term office use.

Device owners bring their devices to use at Wiltshire Council as their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Wiltshire Council is in no way responsible for:

- Personal devices that are broken while at work or during work-sponsored activities
- Personal devices that are lost or stolen at work or whilst undertaking work-related activities
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)
- The management or creation of users own 'cloud' based user accounts, which are required for purchasing software, or backing up data

Wiltshire Council does not guarantee that Service will be compatible with your equipment, or warrant that the Service will be available at all times, uninterrupted, error-free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best Service it can.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates as a result of the use of Wiltshire Council supplied applications as you will not be reimbursed by Wiltshire Council. Finally, Wiltshire Council reserves the right, at its own discretion, to remove any Wiltshire Council supplied applications from your personal device as a result of an actual or deemed violation of the Wiltshire Council's BYOD Policy.

Appendix 1

Wiltshire Council policies and UK Primary legislation

Relevant Wiltshire Council policies:

- Wiltshire Council Information Assurance Acceptable Usage Policy for E-mail, Internet and Computer Use
- Information Security Policy
- Protective Marking Policy
- Social Media and Blogging Policy
- Smartphone – Information Security Procedures
- Data Transfer Procedures
- Information Security Incident Reporting Procedures
- Wiltshire Council Flexible Working Policy and Procedures
- Wiltshire Council Corporate Health and Safety Policy
- Wiltshire Council Disciplinary Policy and Procedure

UK Primary Legislation that may apply:

- Computer Misuse Act 1990
- Data Protection Act 1998 (the DPA)
- Freedom of Information Act 2000
- Caldicott Report 1997
- The Police and Criminal Evidence Act 1984 (Codes of Practice) Order 2008
- Official Secrets Act 1989
- Regulation of Investigatory Powers Act (RIPA) 2000

Appendix 2

Bring Your Own Device Application Form and Acceptable Use Statement

Please return a signed copy of appendix 1 to the ICT Service Desk.

I, _____, the device owner and user, request permission to use my _____ to access Wiltshire Council data and use Wiltshire Council applications as part of flexible working arrangements. I confirm that my device is running on version _____ and meets the minimum system requirement listed in this document.

I have read, understood and agree to respect and follows Wiltshire Council's policies concerning use of these devices and services, as documented in the Bring Your Own Device Policy statement. Further, I have understood the limitations of this IT Service and the consequences of misuse on my behalf.

(Print your name) Signature Date

For use by the ICT Service Desk

SR No.: _____

Date Signed Form returned to Information Services: _____

Date Mobile Device Management enabled: _____