Council Members Policy Document

RBC Bring Your Own Device Policy

Version 1.2

Document Control

Organisation	Redditch Borough Council
Owner	ICT Transformation Manager
Protective Marking	Not protected
Review date	One year from last approval

Revision History

Revision Date	Reviser	Version	Description of Revision
11/03/2019	Peter Bailey	1.0	Policy created
20/03/2019	Peter Bailey	1.1	Initial wording review, signature field
25/04/2019	Peter Bailey	1.2	Second wording review, signature field

Document Approvals

Sponsor Approval	Name	Date	Version Approved

Document Distribution

This document will be distributed via Democratic Services to all Council Members. For those without access to NetConsent the Policy can be signed and returned to the Information Management Team directly or via Democratic Services.

CONTENTS

1. Policy Summary

This policy covers any person wishing to use a device owned by someone other than the Council (e.g. personal devices) to access Council data – commonly known as Bring Your Own Device (BYOD). You must comply with the whole policy, but in summary:

- If you have accepted certain policies and your device meets certain criteria, you may access Council data from a personal device
- **The Council retains control of the council data**, and as part of this agreement you accept the installation of software that can erase Council data from your device and adds certain management facilities for Council use which include being able to record use of facilities
- **You must tell the ICT Helpdesk** if your device is lost, stolen, sold, infected with malware or the security of the device is otherwise compromised or no longer in your possession.
- **The Council does not offer support of the physical personal device** although installation instructions are maintained for your use. The Council will accept comments and issues around BYOD but does not commit to respond to them. Issues with connectivity will be investigated, but if they cannot be reproduced you will have to find solutions in conjunction with your personal providers.
- **Some types of data should not be stored or accessed on BYOD devices for example DWP data. It is your responsibility to be aware of any third-party agreements that you have agreed to.** If you are using as part of your role data from certain partners, you cannot use BYOD devices.

2. Introduction

The Council has a responsibility to safeguard the information that has been provided to it by people and various government and statutory organisations to carry out its business. In order to do this, we need to make sure that:

- the requirements of UK law on personal data management are being met.
- the requirements of the Public Service Network Code of Connection (CoCo) are met
- the Council's own Data Privacy and Information Security policies are being followed
- where third party data is being used, the requirements of the data owners are being followed.

The Council recognises that users may wish to use their own mobile devices to access Council data and use Council applications as part of flexible working

arrangements. This policy outlines the responsibilities of both the device owner and the Council.

3. Who does the Policy apply to?

This policy applies to all persons who connect or intend to connect a device not owned by the Council to use Council data.

4. The Council's Responsibilities

It is the Councils responsibility to provide the Blackberry software license. This can only be done once a cost code and confirmation of policy acceptance is provided via the relevant request form.

It is the Councils responsibility to filter and monitor resources that are available or accessed via the secure Blackberry applications. Activities outside of the Blackberry applications are not captured, stored or monitored by the Council.

It is not the Councils responsibility to reimburse the Council Member for the cost of mobile data, mobile repairs, peripherals, insurance or mobile maintenance of any kind.

As the data controller, the Council is responsible for ensuring that all processing of personal data which is under its control remains in compliance with UK law. Additionally, the Council receives data from partners which may be restricted by their security policies with which we have to comply.

The 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 and consider your rights as an individual to privacy. Decisions on these matters will be made via the Council's internal governance routes.

5. Rights, Privileges and Responsibilities

The use of a personally-owned device in connection with Council business is a privilege granted to device owners. The Council reserves the right to revoke these privileges without notice.

You must read and understand this policy before configuring your device to access Council information.

You must also have completed the Council's training on Data Protection, Freedom of Information and Information Security and have read and accepted the ICT Information Security Policy within the last 12 months of being provided access to information from your personal device.

There are additional requirements for certain persons e.g. contractor staff who may need to sign additional agreements; please consult with the Information Team if you are in this group.

The Council remains the data controller for all Council data held on BYODs.

Disciplinary and / or **criminal action** may be taken **against you** if a breach of policy or law occurs.

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

- You will not lend anyone your device to access Council information or use Council infrastructure.
- Should you decide to sell, recycle, give away or change your device, you will inform the ICT Helpdesk by phone on ext. 1766 or if calling from an external number on 01527 881766. **Do not allow the device to leave your possession until you have been informed council data has been wiped**.
- In accepting this policy, you must ensure that your device has, at minimum, a four-digit pin or a passcode to access your device.
- In order to access your Council e-mail and calendar, you will need to enter your network account password during setup.
- 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 and potentially be wiped of Council data.
- The Council data can be wiped from the device without notice if:
    1) you lose the device;
    2) the device is stolen;
    3) your council membership ends;
    4) ICT detects a data or policy breach or virus/malware infection;
    5) Your device becomes jailbroken or rooted (either intentionally or through the installation of software or an application that makes the modification to add additional functionality)
    6) The device has not connected to the Council infrastructure for 30 days
    7) OS out of date
    8) Deemed necessary by the Council.
- You are responsible for the safekeeping of your own personal data. We recommend that you secure and encrypt your phone appropriately using the facilities on the device, and that you have an up-to-date malware scanning solution installed (anti-virus).
- You must conform strictly to the Council's Information Security Policy.

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 even if this adds additional functionality.

6. Which devices are covered?

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

- Android 6.0 (“Marshmallow”) or higher Smart Phones and Tablets
- iOS 11.0 or higher iPhones and iPad

Devices below these specifications will not comply with our policies and therefore will not be allowed to be used as BYOD.

It should be noted that as technology improves and newer versions of operating system are introduced by vendors or vulnerabilities are discovered in existing operating systems this list is subject to immediate change and access maybe revoked (in some instances this may be without notice).

7. Which Services Are Available via Blackberry Applications?

Currently, the only Services available and covered by this policy are:

- E-mail
- Calendar
- Contacts
- Tasks
- Network file access and editing
- Whitelisted Intranet Sites

Note that some file types cannot be securely opened, and hence you may find you cannot open certain attachments etc.

A minimum four-digit passcode will be required to access devices containing Council data; you will also initially need to set up the device using your Council username/email and password. You **MUST NOT** share these with any other person.

Council data is stored encrypted to protect it and is subject to restrictions on copying and where it can be saved.

8. Who Manages this Facility?

ICT will manage the BYOD facility, as described within this document, on behalf of the Council.

9. What Support will ICT provide?

The Council makes reasonable endeavours to ensure that your device is not adversely affected and that only Council data is erased, but this cannot be guaranteed, and the Council accepts no liability for issues resulting from use. **The Council does not offer support of the physical personal device** although installation instructions are maintained for your use. Furthermore, the Council will not cover any damage to the device or any loss of personal data that may occur as a result of use of BYOD or as part of the removal of Council data.

It is recommended that device owners insure their device as part of their home contents insurance or via a specific mobile device insurance scheme and advise their insurer that the device will be used for work purposes at home and at work locations.

Upon installation of the mobile device management software, the device owner can connect to the Council infrastructure to access their Council accessible data. However, the device owner is personally liable for the device and carrier service costs. They will not be reimbursed by the 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 Council services listed in this document.

10. If a Security incident should occur

A Security incident is defined in the ICT Information Security Policy and can be generally described as **any** event that could compromise information security. Some examples: your device is lost or stolen, someone else gains access to your password/passcode, your device becomes infected with malware.

If a security incident should occur, you are required to inform the Information Management Team and your Line Manager **immediately** with details.

The Council reserves the right to wipe Council data and applications.

You should ensure that you read and understand both the policy and your responsibilities to report a security incident. In all cases you should contact the Information Management Team directly or via the ICT Helpdesk.

The Council also needs to act where potential incidents are identified. Where ‘near misses’ occur, these should be reported to Information Management Team and a local decision taken as to whether the cause of the ‘near miss’ is one which could involve the enhancement of the policy or the process. If this

is the case, you should contact the Information Management Team directly or via the ICT Helpdesk.

Note that not immediately reporting security incidents is a breach of this policy.

11. ICT Services Security Incident Response

When a security incident is reported ICT Services are required to remove the Council data and application from the affected device.

12. Guidelines for Acceptable Behaviour

Device owners are expected to behave in accordance with the Council's policies whilst undertaking work for the Council. Further information can be provided by your manager or by contacting a 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. Your data and device could be examined by other parties in any legal action.

13. Allowed Countries

The General Data Protection Regulation only permits export of personal data to certain countries. Because of this, we can only permit BYOD applications with Council data to be accessed within the United Kingdom. Council data is encrypted using the password set by the Council Member in the Blackberry application and **MUST NOT** be entered outside the United Kingdom.

14. If You Leave the Council

Democratic Services are required to inform ICT when you are leaving the council, your access to the Council infrastructure and applications will cease and your device will be de-provisioned, access to Council data will cease and Council data wiped.

15. Council Release of Liability and Disclaimer Statement

The Council hereby acknowledges that the use of a personal device in connection with 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 non-council data, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

The Council hereby disclaims liability for the loss of any such non-council data and/or for service interruptions. The Council expressly reserves the right to wipe the Council application and data at any time as deemed necessary for purposes of protecting or maintaining Council infrastructure and services. The Council also disclaims liability for device owner injuries such as repetitive stress injuries developed; The Council provides ICT equipment that is suitable for long-term office use.

Device owners bring their devices to use at the 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.

The 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

The 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 Council supplied applications as you will not be reimbursed by the Council.

The Council reserves the right, at its own discretion, to remove any Council supplied applications from your personal device as a result of an actual or deemed violation of the Council’s BYOD Policy.

16. Policy Acceptance for Offline Distribution

Please sign and date below to acknowledge that you have read and understand the content above and agree to adhere to the RBC Council Members Policy. **You cannot use a BYOD if you do not read, understand and accept this policy.**

Signed:

Date:

Please return the signed policy document to :-

Democtractic Services
Redditch Borough Council
Town Hall
Walter Stranz Square
Redditch
Worcestershire
B98 8AH