RUSHMOOR BOROUGH COUNCIL




# Bring Your Own Device
# BYOD

*N.B. Staff should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.*

# Contents

# 1. Introduction

1.1 Rushmoor Borough Council (RBC) recognises that employees, Members and contractors ('users') may wish to use their own mobile devices to access council email. This policy outlines the responsibilities of both the device owner and RBC.

1.2 Access and continued use of Council data and applications is granted on the condition that device users read, understand, accept and follow the policies and procedures contained within this document. RBC reserves the right to revoke these privileges if device users do not abide by this policy.

# 2. What is BYOD?

BYOD refers to any person wishing to use a device owned by someone other than the Council in order to access Council data. The Council can provide access to Outlook email, contacts and calendar through a secure application on your own device. This policy applies to any user making use of this application.

# 3. Which devices are covered?

3.1 Current devices approved for BYOD are Android phones and tablets, iPhones and iPads. Users must ensure that devices are kept up to date with the latest operating system. *Because Android devices are less secure than iPhones and iPads, users are required to have anti-malware software installed on their devices.*

3.2 As technology improves and newer versions of operating systems are introduced, or vulnerabilities are discovered in existing operating systems then devices should be updated. If not updated, then the device will be deemed as non-compliant and access will be revoked without notice.

# 4. Device user responsibilities

4.1 As the user of a device covered by this Policy; you carry specific responsibilities as detailed below:

- You will not lend anyone your device to access RBC data.
- Should you sell, recycle, or give away your device, you must notify the IT Service Desk immediately. Failure to do so may result in a loss of Council data and may result in disciplinary action.
- You should have a 6-digit pin or fingerprint to access your device. In any event, the user will still have to enter a secure PIN or biometric log on to access the application.
- The application, to access the Council email, is required to automatically lock every 5 minutes of inactivity and will require you to re-enter your pin.
- In order to setup your device to access your work outlook email, calendar and contacts you will need to enter your network account password. You will be required to change this every 90 days.
- You are responsible for the safekeeping of your own personal data and ensuring that it is backed up.
- Any sensitive information should not be emailed via your mobile device, as it will not be secure. A Council owned and managed Laptop or PC should be used.
- You must ensure that your device is compliant with the system requirements (detailed above) and that security software is kept up to date. Checks will be carried

out by the application software to ensure that your device meets the compliance criteria and if not, the application will automatically stop synchronising.

- You must not use your device to store corporate emails, files or data.
- If any of the following events occur:
  - The device is lost or stolen (which must be reported immediately you become aware)
  - Your employment is terminated without notice
  - You terminate your employment (after your notice period has expired)
  - IT Services detect a data or policy breach or virus,

  IT Services will wipe all Council related data from the device. In so doing, there is a risk that ALL data on the mobile device may be wiped
- 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. Any devices that become rooted or jail broken will automatically stop synchronising and will be reported to the IT Service Desk.
- All users are responsible for any backups of their data.
- All users must comply with GDPR and Data Protection Act 2018 and Council guidance when using any personal device for work.

## 5. RBC's responsibility

5.1 As the data controller, RBC is responsible for ensuring that all processing for personal data which is under its control remains in compliance with the Data Protection legislation.

## 6. Security incidents

6.1 Several security incidents (data breaches) could occur when using personal devices with RBC's data. If a security incident should occur, e.g. your device is lost or stolen, you must notify your manager - Members should notify the Head of Finance, the Data Protection Officer and the IT Service desk, in line with the Council's Data Protection Breach Policy

6.2 In the event of any security incidents, IT Services reserve the right to wipe either RBC data or the whole device, if it is deemed necessary. This may impact on the applications and personal data stored on your device. Therefore, it is key to ensure that you regularly back up your device on your own personal laptop.

## 7. Process for requesting access to BYOD

7.1 Requests for BYOD should be made through the IT Service Desk. This policy must be read, and the policy statement in appendix A signed to show acceptance of adhering to the requirements detailed within this policy. An electronic copy of the signed policy statement will be retained.

7.2 Upon receipt of the signed policy statement, the IT Service Desk will decide with you to apply the BYOD software onto your device. For Android devices if anti-virus software is not on your device then this will be installed at this stage prior to the BYOD software being put onto your device.

## 8. RBC's release of liability and disclaimer statement

8.1 Rushmoor Borough Council (RBC) herby acknowledges that the use of a personal device in connection with RBC business carries specific risks for which you, as the device owner and user must 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.

8.2 RBC hereby disclaims liability for the loss of any such data and/or for service interruptions. RBC 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 RBC infrastructure and services.

8.3 RBC also disclaims liability for device owner injuries such as repetitive strain injuries developed. RBC provides IT equipment that is suitable for long-term office use.

8.4 Device users use them at RBC at their own risk. Device users 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.

8.5 Device users should be aware that any personal device used at work may be used as evidence in legal action involving the Council. This means that your data could be examined not only by Rushmoor Borough Council but also by other parties involved in the legal action.

8.6 RBC will in no way accept responsibility for the following:

- Personal devices that are broken at work or during work related 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.

8.7 RBC does not guarantee that service will be compatible with your equipment or warrant that the service will always be available, uninterrupted, error free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best service it can.

8.8 RBC will not reimburse any costs associated with the running or maintenance of the mobile device.

8.9 RBC reserves the right, at its discretion, to remove any RBC supplied applications from your personal device as a result of an actual or deemed violation of this policy.

## Appendix A

**Please return a signed copy to the IT Service Desk**

I request permission to use my …….to access Rushmoor Borough Council data. I confirm that my device meets the minimum system requirements listed within this document.

I have read, understood and agree to follow Rushmoor Borough Council's policy concerning use of my device(s), as detailed within this policy. Furthermore, I understand the limitations of this service and the consequences of any misuse.

Print your name ……

Signature ……

Date ……

---

For use by IT service desk:

Data software enabled on the device ……

Device details ……

Minimum requirements met: Y/N