SALISBURY
CITY COUNCIL

Bring Your Own Device (BYOD) Policy

Policy Number	Version	Owner	Doc No.	PDF No.	Date Published	Review Due	Review Team
XXXX	1	CSM	XXXXX	XXXXX	December ‘19		Management

Distribution

Internal: Salisbury City Council Councillors

External: Blue Frontier

Contents

1. Introduction

1.1. Salisbury City Council (the council) supports the use of personal devices such as laptops, smartphones and tablets, to enable access to council information. Using a personal device in this way is called Bring Your Own Device (BYOD).

1.2. There are increased information risks associated with BYOD, such as making sure that council information is kept secure even if your personal device is lost or stolen, or is used by another person.

2. Purpose

2.1. This policy is intended to reduce the risks of BYOD by clearly outlining individual responsibilities, minimum requirements, and acceptable use.

2.2. This policy is for all members who access the council's information using a personal device.

2.3. Breach of this, or the Members Code of Conduct may result in loss of BYOD access.

3. Supported Devices

3.1. The most recent versions of Android and IOS are supported for BYOD at Salisbury City Council.

3.2. Other devices and older versions of Android and IOS are not supported for BYOD, because they do not meet the required security standards.

3.3. Rooted or jail-broken devices will not be enabled for BYOD use. Any device that becomes rooted or jail broken will have access denied or removed.

4. Available Services

4.1. The services available for BYOD will depend on current technology and network constraints. Members have access to Salisbury City Council's secure email servers via Outlook Web Access.

4.2. Other services may be restricted by the constraints of your personal device, or might require additional apps to be downloaded.

5. Device Owner Responsibilities

5.1. If you use your personal device to access council information, you are responsible for protecting the device. This includes ensuring the device is not used by anyone else to gain access to council information – even if you think the information is not confidential.

5.2. Device owners are expected to behave in accordance with Salisbury City Councils Members Code of Conduct whilst using personal devices to work for the Council.

5.3. We strongly recommend that you set a pin of at least 4 digits to unlock your phone as a minimum. Using an additional step such as your fingerprint will improve the security of your phone.

5.4. As the device owner, you have some specific responsibilities:

5.4.1. Do not lend anyone your device to access Salisbury City Council information or networks;

5.4.2. Notify the Corporate Service Manager before you sell, recycle, give away or otherwise dispose of your device, to allow access to council information to be removed securely by our IT support provided Blue Frontier;

5.4.3. Any private information or applications on the phone are entirely your own responsibility;

5.4.4. Adhere to the councils Members Code of Conduct and Social Media Guidance for Members when you use your personal device for BYOD;

5.4.5. Always take appropriate steps to maintain the security of Salisbury City Council information;

5.4.6. Do not try to download council information or files to your mobile device;

5.5. If you need to email sensitive or confidential information to an external recipient, then the information must be password-protected and encrypted. If you are unable to do this, do not send the email using your personal device;

5.6. Ensure that your device is compliant and that security software is up-to-date. If your personal device no longer meets the minimum requirements required to access council information securely, that access will be removed automatically;

5.7. Report the loss or theft of your personal device to the Corporate Services Manger immediately. Blue Frontier will remotely remove access to council information;

5.8. If you think that your access to council information has been misused, or that council information has been breached or shared inappropriately, you must notify the Corporate Services Manger immediately. Blue Frontier will remotely remove access to council information;

5.9. You are responsible for the safekeeping of your own personal data;

5.10. You will be responsible for paying any network charges you might incur whilst using your personal device for BYOD;

5.11. You should use your phone in an ethical manner. Any device which is jailbroken, rooted, or otherwise modified beyond the routine installation of updates as directly provided by the manufacturer or mobile operator will automatically lose access to council information.

5.12. It is recommended that you insure your personal device under your home contents or other insurance.

5.13. Any personal device used for council use may be subject to “discovery in litigation”. This means that it could be used as evidence in a lawsuit against Salisbury City Council. Your data could be examined not only by Salisbury City Council but also by other parties in any lawsuit.

6. Salisbury City Council Responsibilities

6.1. As a data controller, Salisbury City Council is responsible for ensuring that all processing of personal data which is under its control, remains in compliance with the General Data Protection Regulation 2016 (GDPR).

6.2. Salisbury City Council will respect the privacy rights of individuals and only implement security measures which are required to meet its obligations as a data controller.

6.3. Salisbury City Council will not be responsible for covering the costs of damage to, or loss of, any personal device used for BYOD.

6.4. Salisbury City Council will not be responsible for covering any network costs incurred when using a personal device for BYOD.

7. Blue Frontier Responsibilities

7.1. Salisbury City Councils IT support provider Blue Frontier will manage the BYOD facility, ensuring appropriate security is in place, and that only suitable devices can connect.

7.2. Blue Frontier will not be responsible for maintaining any personal device used for BYOD.

7.3. Blue Frontier will remove access from personal devices which have not connected to Salisbury City Council Outlook Web Access for more than 30 days. Device access will also be removed in the event of a member leaving Salisbury City Council.

8. Information Incidents

8.1. In the event of an information incident, you are required to inform the Corporate Service Manager or Blue Frontier immediately with details. **You will be asked to complete a Data Breach Incident Report Form.**

8.2. The council will work with Blue Frontier to manage the incident, and will advise you of any other required action. It is important to get advice from the Corporate Services Manger prior to taking any steps to address the situation, so that an appropriate response can be agreed.

8.3. Depending on the severity of any information incident, the council may need to immediately restrict your BYOD access to council systems.

9. Monitoring

9.1. BYOD access will be automatically monitored to ensure that personal devices are kept up-to-date and are secure. Any personal device which does not meet security requirements will have BYOD access remotely removed.

9.2. In the event of any misuse of BYOD access, the Corporate Services Manager will be informed.

9.2.1. The council cannot and will not monitor the private usage of your phone.

9.3. Relevant Documents and Further Information

Members Code of Conduct

Social Media Guidance for Member

Members Communications and Data Protection Guidance

Data Breach Incident Report Form

Further information regarding BOYD guidance can be found on The Information Commissioners office (ICO) website https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf