

COMMITTEE REPORT

Subject:	<i>Bring Your Own Device (BYOD) Policy</i>
Committee:	<i>Governance, Policy & HR Committee</i>
Item Number:	<i>10</i>
Date:	<i>5 October 2026</i>
Author:	<i>Jeremy Cotton, IT Manager</i>
Report status:	<i>Decision</i>
Confidential / Exempt:	<i>No</i>

1. Report Summary

This report presents the review and proposed update of the Council's Bring Your Own Device (BYOD) Policy for members and officers. The review updates the policy to reflect current device-security, Microsoft 365 and IT support arrangements while retaining its existing purpose and overall control framework.

- 1.1 The purpose of this report is to seek Committee approval of the revised Bring Your Own Device (BYOD) Policy at Appendix A.
- 1.2 The policy is classified as a Type 2 policy under the Council's Policy and Procedures Management Policy and is therefore subject to review at least every three years, or sooner where legislative, technological or operational changes require it.
- 1.3 In accordance with the requirements of AGAR Assertion 10 and the Council's arrangements for secure IT and data management, Council business must be conducted using Council-provided email accounts. Members and officers must use their @salisburycitycouncil.gov.uk email address for Council correspondence and must not use personal email accounts for Council business. Where a member or officer accesses Council email, systems or information using a personally owned device, the requirements of this policy apply.
- 1.4 The review updates wording on supported devices and security controls, Microsoft 365 access, removal of Council access from personal devices, IT support responsibilities and related documents. Outdated references to Outlook Web Access and the previous 30-day inactivity arrangement are removed.
- 1.5 The update is being brought forward so that members and officers have a policy which reflects the controls and support arrangements currently used when Council information is accessed from a personal device.

- 1.6 The Committee is asked to approve the revised policy. A clean copy is provided at Appendix A, and a marked-up copy showing the proposed amendments is provided at Appendix B.

2. Recommendations

It is recommended that the Committee:

- 2.1 To approve the revised Bring Your Own Device (BYOD) Policy at Appendix A.

3. Background

- 3.1 The Council's Bring Your Own Device (BYOD) Policy for Members was published in December 2019 and applies where Members use personal laptops, smartphones or tablets to access Council information.
- 3.2 The policy sets minimum requirements and responsibilities intended to reduce information-security risks associated with using a personal device for Council business. It covers supported devices, Member responsibilities, Council and IT support responsibilities, information incidents and monitoring.
- 3.3 Under the Council's Policy and Procedures Management Policy, the BYOD Policy is treated as a Type 2 policy and is subject to a three-year review cycle, with earlier review where required by changes in legislation, technology or operational practice.

4. Proposal

- 4.1 The revised policy at Appendix A is proposed to replace the current version following approval.
- 4.2 The review has been undertaken to ensure that the policy reflects current technical controls and support arrangements rather than legacy systems or processes.
- 4.3 The changes update device-support and security wording, clarify Microsoft 365 application PIN requirements, remove outdated system-specific wording, clarify the roles of the IT Manager and IT support provider, and update the list of related documents. The core user responsibilities and information-security controls remain in place.
- 4.4 The update is required now because the existing policy contains technical and operational references that no longer accurately describe the arrangements used by the Council.
- 4.5 The updated policy applies to both members and officers where they use personally owned devices to access Council information, systems or services.

5. Financial Position

- 5.1 No additional expenditure is proposed as a result of the policy update.
- 5.2 Existing IT support and administration arrangements will continue to be met from existing resources.
- 5.3 No additional staffing, maintenance costs or future financial liabilities are identified by this policy review.
- 5.4 The proposal is a governance and policy update and does not require a separate value-for-money assessment.

6. Legal and Governance Considerations

- 6.1 Section 111 of the Local Government Act 1972 enables the Council to take steps calculated to facilitate, or which are conducive or incidental to, the discharge of its functions. This supports the maintenance of appropriate internal governance and information-security arrangements.
- 6.2 The policy also supports the Council's responsibilities under the UK General Data Protection Regulation and the Data Protection Act 2018 by setting controls around access to Council information from personal devices.
- 6.3 AGAR Assertion 10 addresses digital and data compliance. The 2026/27 Practitioners' Guide requires every authority to have a generic email account hosted on an authority-owned domain and requires smaller authorities, excluding parish meetings, to have an IT policy covering the secure and lawful use of both authority-owned and personal IT equipment. The Guide also provides that an authority's IT policy should mandate the use of authority-owned email accounts for official business. The revised BYOD Policy supports these requirements by setting controls for members and officers accessing Council email, systems or information from personally owned devices.
- 6.4 The matter is brought to the Governance, Policy & HR Committee for approval as a Type 2 policy in accordance with the Council's Policy and Procedures Management Policy.
- 6.5 Keeping the policy current reduces governance and information-security risk arising from members and officers relying on outdated technical or support instructions.

7. Consultation and Engagement

- 7.1 No public consultation is required for this review because the policy concerns the internal use of personal devices by members and officers to access Council information, systems and services.
- 7.2 The proposed clean policy and marked-up version are presented together so that Members can see both the policy proposed for approval and the changes made during the review.
- 7.3 No external consultation has been undertaken because the changes relate to internal governance, information security and IT support arrangements.
- 7.4 Follow up with staff and member awareness of the policy.

8. Strategic and Policy Alignment

- 8.1 The revised policy supports effective corporate governance and the secure handling of Council information when members and officers use personal devices.
- 8.2 It aligns with the Council's Policy and Procedures Management Policy and with the Member conduct, communications, social media and data-protection documents referenced within the BYOD Policy.

9. Implementation and Next Steps

- 9.1 Subject to the Committee's decision, the next steps will be as follows:
 - 9.1.1 Finalise the policy version, approval date and review information.
 - 9.1.2 Issue the approved policy as the controlled version and circulate it to members and

officers.

9.1.3 Support officers and members to secure devices if new/further risks identified.

9.1.4 Archive the superseded policy in accordance with the Council's policy-management arrangements.

9.1.5 Review the revised policy in accordance with the Policy and Procedure Management Policy.

9.2 Responsibility for implementation will sit with Corporate Services, with the IT Manager responsible for the operational BYOD controls described in the policy.

10. Additional Relevant Information

10.1 Appendix A is the clean policy proposed for approval. Appendix B is the comparison copy showing the amendments in context: red text identifies new or amended wording and red strikethrough identifies wording proposed for deletion.

11. Implications

Implication Area	Impact	Comments / Mitigation
Financial	None	No additional expenditure is proposed; existing resources and IT support arrangements continue.
Legal	Low	The policy supports internal governance and data-protection responsibilities; section 111 Local Government Act 1972 is the supporting power identified for this action.
Risk	Medium	BYOD information-security risks are mitigated through device standards, access controls and prompt incident reporting.
Personnel	None	No staffing changes are proposed.
Environmental Impact	None	No material environmental impact is identified.
Equalities Impact Statement	None	No specific equalities impact is identified; the policy applies consistently to Members using BYOD.
Community / Public Impact	None	No direct impact on public service delivery is identified.
Procurement / Contractual	None	No new procurement or contractual commitment is proposed.
Property / Asset	None	Personal devices remain the responsibility of their owners.
Data Protection	Medium	The policy sets controls intended to reduce unauthorised access, loss or inappropriate disclosure of Council information.

12. Appendices / Background Papers

12.1 Appendix A - Proposed revised Bring Your Own Device (BYOD) Policy

12.2 Appendix B - Proposed revised Bring Your Own Device (BYOD) Policy marked-up copy showing changes

Appendix A



Bring Your Own Device (BYOD) Policy

Policy Number	Version	Owner	Date Published	Review Due	Review Team
CORP/PO/019	1	CSM	September 2026	September 2029	Management

Distribution

Internal: Salisbury City Council & Councillors
External: Blue Frontier

Contents

- 1. Introduction**
- 2. Purpose**
- 3. Supported Devices**
- 4. Available Services**
- 5. Device Owner Responsibilities**
- 6. Salisbury City Council Responsibilities**
- 7. IT Support Responsibilities**
- 8. Information Incidents**
- 9. Monitoring**
- 10. Relevant Documents and Information**

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, 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 applies to all members and officers who access Council information, systems or services using a personally owned device.
- 2.3. A breach of this policy may result in BYOD access being restricted or removed and may be dealt with under any other relevant Council policy, code or procedure.
- 2.4. Council business must be conducted using Council-provided accounts. Members and officers must use their @salisburycitycouncil.gov.uk email account for Council correspondence and must not use personal email accounts for Council business.

3. Supported Devices

- 3.1. Supported versions of Android and iOS that meet the Council's security requirements may be used for BYOD.
- 3.2. Other devices and older versions of Android and IOS may not be supported for BYOD, because they do not meet the required security standards. The versions deemed to introduce unacceptable risk will be reviewed by the IT Manager and communicated to affected users in a timely manner.
- 3.3. Rooted or jailbroken devices will not be enabled for BYOD use. Any device that becomes rooted or jail broken will have access denied or removed.
- 3.4. Devices used for BYOD must comply with the Council's security controls, including device-management requirements where applicable.
- 3.5. The Council and its IT support provider are not responsible for the general maintenance or support of personally owned devices.

4. Available Services

- 4.1. The services available for BYOD will depend on current technology and network constraints.
- 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. Users must comply with all relevant Council policies, codes and guidance when using a personal device for Council business. Members must also comply with the Members' Code of Conduct.
- 5.3. Application PINs are enforced on devices when accessing SCC accounts through M365 apps. For example, Using the Outlook app for SCC will enforce PIN protection regardless of whether there is or isn't a personal account already set up.
- 5.4. As the device owner, you have some specific responsibilities:
 - 5.4.1. Do not permit another person to use your device to access Council information, systems or networks;
 - 5.4.2. Notify the IT Manager before you sell, recycle, give away or otherwise dispose of your device, to allow access to council information to be removed securely;
 - 5.4.3. Any private information or applications on the devices are entirely your own responsibility;
 - 5.4.4. Comply with all relevant Council policies, codes and guidance when using your personal device for Council business;
 - 5.4.5. Always take appropriate steps to maintain the security of Salisbury City Council information;
 - 5.4.6. Council information must not be intentionally downloaded or stored locally on a personal 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 the device operating system, applications and required security controls are supported and kept 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 IT Manager immediately. Council access and/or Council-managed data may be remotely removed where appropriate and technically possible.
- 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 IT Manager immediately. Council access and/or Council-managed data may be remotely removed where appropriate and technically possible.
- 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. Council information accessed or held on a personal device remains subject to applicable legal and information-governance requirements. Where required by law, relevant Council information may need to be identified, preserved, retrieved or disclosed, including in connection with legal proceedings or statutory information-rights requests.

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 UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- 6.2. The Council will respect individuals' privacy rights and implement proportionate security measures necessary to meet its legal and information-security obligations.
- 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. IT Support Responsibilities

- 7.1. The Council's IT Manager and appointed IT support provider will manage the BYOD arrangements ensuring appropriate security is in place, and that only suitable devices can connect.

- 7.2. Neither the Council nor its IT support provider is responsible for maintaining personally owned devices used for BYOD.
- 7.3. BYOD access will be removed when a member or officer ceases to require access to Council systems, including when they leave the Council.

8. Information Incidents

- 8.1. In the event of an information incident, you are required to inform the IT Manager or Blue Frontier immediately with details. **You will be asked to complete a Data Breach Incident Report Form.**
- 8.2. The IT Manager will work with IT support provider to manage the incident, and will advise you of any other required action. It is important to get advice from the IT Manager 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 may be monitored to confirm compliance with the Council's security requirements. Access may be restricted or removed where those requirements are not met.
- 9.2. In the event of any misuse of BYOD access, the IT Manager will be informed.
 - 9.2.1. The Council's BYOD controls are not intended to monitor users' private use or personal content on their devices.

9.3. Relevant Documents and Further Information

- Members Code of Conduct
- Social Media Guidance for Member
- Data Breach Incident Report Form
- Mobile Phone Policy
- E-Safety and Online Behaviours Policy
- Acceptable Use and Asset Management Policy
- 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

Appendix B



Bring Your Own Device (BYOD) Policy

Policy Number	Version	Owner	Doc No.	PDF No.	Date Published	Review Due	Review Team
CORP/PO/019	1	CSM IT Manager	XXXXX	XXXXX	December '19 September 2026	September 2029	Management

Distribution

Internal: Salisbury City Council & Councillors

External: Blue Frontier

Contents

- 1. Introduction**
- 2. Purpose**
- 3. Supported Devices**
- 4. Available Services**
- 5. Device Owner Responsibilities**
- 6. Salisbury City Council Responsibilities**
- 7. ~~Blue-Frontier~~ IT Support Responsibilities**
- 8. Information Incidents**
- 9. Monitoring**
- 10. Relevant Documents and Information**

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.~~ This policy applies to all members and officers who access Council information, systems or services using a personally owned device.
- 2.3. ~~Breach of this, or the Members Code of Conduct may result in loss of BYOD access.~~ A breach of this policy may result in BYOD access being restricted or removed and may be dealt with under any other relevant Council policy, code or procedure.
- 2.4. Council business must be conducted using Council-provided accounts. Members and officers must use their @salisburycitycouncil.gov.uk email account for Council correspondence and must not use personal email accounts for Council business.

3. Supported Devices

- 3.1. ~~The most recent versions of Android and iOS are supported for BYOD at Salisbury City Council.~~ Supported versions of Android and iOS that meet the Council's security requirements may be used for BYOD.
- 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~~ may not be supported for BYOD, because they do not meet the required security standards. The versions deemed to introduce unacceptable risk will be reviewed by the IT Manager and communicated to affected users in a timely manner.
- 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.
- 3.4. ~~Devices used for BYOD must comply with the Council's security controls, including device-management requirements where applicable.~~
- 3.5. ~~The Council and its IT support provider are not responsible for the general maintenance or support of personally owned devices.~~

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 Council's Members Code of Conduct whilst using personal devices to work for the Council. Users must comply with all relevant Council policies, codes and guidance when using a personal device for Council business. Members must also comply with the Members' Code of Conduct.~~
- 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.~~ Application PINs are enforced on devices when accessing SCC accounts through M365 apps. EG: Using the Outlook app for SCC will enforce PIN protection regardless of whether there is or isn't a personal account already set up.
- 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; Do not permit another person to use your device to access Council information, systems or networks.~~
 - 5.4.2. Notify the [IT 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 devices](#) 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; Comply with all relevant Council policies, codes and guidance when using your personal device for Council business.~~
 - 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; Council information must not be intentionally downloaded or stored locally on a personal 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.~~ Ensure that the device operating system, applications and required security controls are supported and kept 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 [IT Manager](#) immediately. ~~Council access and/or Council-managed data may be remotely removed where appropriate and technically possible;~~
- ~~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 [IT Manager](#) immediately. ~~SCG data will be removed remotely; Blue Frontier will remotely remove access to council information; Council-managed data may be remotely removed where appropriate and technically possible;~~
- 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. Council information accessed or held on a personal device remains subject to applicable legal and information-governance requirements. Where required by law, relevant Council information may need to be identified, preserved, retrieved or disclosed, including in connection with legal proceedings or statutory information-rights requests.~~

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).~~ UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- 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.~~ The Council will respect individuals' privacy rights and implement proportionate security measures necessary to meet its legal and information-security obligations.
- 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~~ IT Support Responsibilities

- 7.1. ~~Salisbury City Council's~~ The Council's IT Manager and support provider ~~Blue Frontier~~ will manage the BYOD facility, ensuring appropriate security is in place, and that only suitable devices can connect.
- 7.2. Neither ~~SCC nor Blue Frontier are~~ the Council nor its IT support provider is 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.~~ BYOD access will be removed when a member or officer ceases to require access to Council systems, including when they leave the Council.

8. Information Incidents

- 8.1. In the event of an information incident, you are required to inform the IT Manager or Blue Frontier immediately with details. **You will be asked to complete a Data Breach Incident Report Form.**
- 8.2. The IT Manager will work with ~~Blue Frontier~~ the IT support provider to manage the incident, and will advise you of any other required action. It is important to get advice from the IT Manager 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~~ **may** 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.~~ Access may be restricted or removed where those requirements are not met.

9.2. In the event of any misuse of BYOD access, **the IT Manager** will be informed.

9.2.1. ~~The council cannot and will not monitor the private usage of your phone. The Council's BYOD controls are not intended to monitor users' private use or personal content on their devices.~~

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