COMMITTEE REPORT

Subject:	*ICT Acceptable Use and Asset Management Policy*
Committee:	*Governance, Policy & HR Committee*
Item Number:	*12*
Date:	*5 October 2026*
Author:	*Jeremy Cotton, IT Manager*
Report status:	*Decision*
Confidential / Exempt:	*No*

1. Report Summary

This report presents a new ICT Acceptable Use and Asset Management Policy for members and staff. The policy brings together the standards for use of Salisbury City Council (SCC) ICT systems with the controls for issuing, protecting, recording, monitoring and returning Council-owned ICT equipment.

1.1 The purpose of this report is to seek Committee approval of the ICT Acceptable Use and Asset Management Policy at Appendix A.

1.2 The policy is classified as a Type 2 policy under the Council's Policy and Procedures Management Policy. Type 2 policies are reviewed at least every three years, or sooner where required.

1.3 The policy applies to employees (officers), members, contractors, agency staff and third parties accessing SCC systems. It covers acceptable use, Council-issued equipment, information security, passwords and authentication, software, remote access, email and Microsoft 365, personal devices, printing, incident reporting, asset management, monitoring and the return of equipment.

1.4 The policy also establishes practical asset-accountability controls, including asset tagging and registration, an annual stock and suitability review, prompt reporting of loss or damage, and a one-chance approach to replacement or repair of lost, stolen or damaged equipment. Staff issue and acknowledgement forms support these arrangements.

2. Recommendations

It is recommended that the Committee:

2.1 To approve the ICT Acceptable Use and Asset Management Policy at Appendix A.

3. Background

3.1 SCC provides staff, members and other authorised users with ICT systems, Microsoft 365 services, email, remote-access facilities and Council-owned equipment to support service delivery. These resources need to be used securely, responsibly and consistently, and Council assets need to remain identifiable, protected and recoverable throughout their lifecycle.

3.2 The new draft policy creates a single corporate framework covering both acceptable use of ICT and management of Council-issued equipment. It defines the responsibilities of users, IT Services and managers and sets expectations for security, data handling, approved software, remote access, incident reporting and equipment care.

3.3 The policy is classified as Type 2 because it is a corporate policy regulating the effective management of the Council. Under the Council's Policy and Procedures Management framework, Type 2 policies are reviewed at least every three years.

4. Proposal

4.1 It is proposed that the Committee approves the ICT Acceptable Use and Asset Management Policy at Appendix A for application to employees (officers), members, contractors, agency staff and third parties accessing SCC systems.

4.2 For acceptable use, the policy states that SCC ICT systems are provided primarily for business purposes, with limited personal use permitted where it does not interfere with work, consume excessive resources or breach Council policy. Users must protect Council data, comply with relevant information-security requirements and avoid activity that could harm SCC systems, information or reputation.

4.3 The policy sets technical and behavioural controls for Council devices and accounts. These include keeping devices secure and connected for updates, using strong passwords and multi-factor authentication where provided, using approved software, accessing systems remotely through approved arrangements, using SCC email for official communications, reporting suspicious communications and not forwarding Council data to personal email accounts.

4.4 Asset management requirements include Council ownership of issued equipment, asset tagging and registration against the user, prompt reporting of faults, loss, theft or damage, annual stock and suitability checks, and return of all equipment when requested or when employment ends. The policy also establishes a one-chance approach to replacement or repair of lost or damaged equipment, with subsequent costs normally falling to the relevant department unless an approved exception applies.

5. Financial Position

5.1 No new budget is requested as a direct consequence of approving the policy. The policy formalises controls that will primarily be delivered through existing IT, HR and departmental arrangements.

5.2 The policy may have financial consequences where Council equipment is lost, stolen or damaged. It provides that SCC may replace or repair a device on the first occasion without charge to the employee's department, with the full cost of a subsequent incident normally charged to that department unless an approved exception applies.

5.3 Routine asset-management activity, including tagging, maintaining the asset register, stock checks, security controls and replacement of equipment through normal lifecycle

arrangements, will continue to be managed within approved budgets. Any expenditure outside existing provision would require separate approval.

5.4 The policy supports value for money by setting clearer ownership, care and return requirements for ICT assets and by providing a consistent basis for managing avoidable loss or damage.

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 controls for staff use of ICT systems and management of Council assets.

6.2 The policy requires ICT use to comply with relevant legislation identified within the policy, including the UK General Data Protection Regulation, Data Protection Act 2018, Computer Misuse Act and copyright law. It also requires secure handling of personal and sensitive data, controlled software use and immediate reporting of security incidents and suspected data breaches.

6.3 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 framework.

6.4 Monitoring of ICT systems must remain necessary and proportionate for security, compliance, audit, investigation and service-integrity purposes. Implementation should also ensure that staff issue and acknowledgement arrangements, asset records and related operational procedures remain consistent with the approved policy.

7. Consultation and Engagement

7.1 The policy document contains internal comments concerning its scope and wording, including confirmation that it complements the ESafety and Online Behaviours Policy.

7.2 No formal resident or public consultation is identified in the policy. The subject is primarily an internal staff and members acceptable use of SCC systems, devices and networks.

7.3 Follow up with staff and member awareness of the policy.

8. Strategic and Policy Alignment

8.1 The policy supports effective corporate governance, information security, organisational resilience and responsible stewardship of Council assets. It establishes consistent expectations for how ICT systems and devices are used, protected, recorded and returned.

8.2 The policy is intended to operate alongside the Council's ESafety and Online Behaviours Policy, Bring Your Own Device (BYOD) Policy and Data Protection Policy, which are identified as associated policies within the draft.

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 approval date and controlled document information.

9.1.2 Issue the approved policy to staff, members and other relevant users, and implement the associated staff issue and acknowledgement arrangements for Council-owned

devices.

9.1.3 Maintain the asset register, tagging, stock-review, security, incident-reporting and return arrangements set out in the policy.

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

9.2 Responsibility for implementation will sit with the IT Manager, working with HR, line managers and relevant service managers across the Council.

10. Operational Controls and Asset Accountability

10.1 The policy requires Council-issued equipment to remain under SCC ownership, to be recorded against the relevant user and to carry asset identification. Users must take reasonable care of equipment, report faults or incidents promptly and return equipment when requested or when their employment ends. Managers are responsible for ensuring that leavers' equipment is returned to the IT Manager.

10.2 The Mobile Phone Staff Issue Form and the PC, Laptop and Tablet Staff Issue Form support implementation by recording the user's acknowledgement of acceptable use, device care, security, loss or damage and return requirements. These are operational documents supporting the policy rather than separate policy decisions and should be maintained so that they remain consistent with the approved policy.

11. Implications

Implication Area	Impact	Comments / Mitigation
Financial	Low	No new budget is requested. The policy may transfer the cost of subsequent loss or damage to the relevant department and any unbudgeted replacement expenditure will remain subject to normal financial controls.
Legal	Low	The policy establishes internal ICT and asset controls and requires compliance with data-protection, computer-misuse and copyright requirements. Section 111 of the Local Government Act 1972 is the supporting power identified for this action.
Risk	Medium	ICT misuse, insecure data handling, lost equipment and weak asset control can affect systems, information, finances, reputation and service continuity. The policy mitigates these risks through defined user, manager and IT responsibilities.
Personnel	Medium	The policy applies to employees and other authorised users. Staff must comply with acceptable-use, security, incident-reporting and equipment-care requirements; non-compliance may have disciplinary consequences under existing arrangements.
Environmental Impact	Low	The policy encourages minimised printing and structured management of ICT assets. No material adverse environmental impact has been identified.

Equalities Impact Statement	Low	The policy applies consistently to staff and other authorised users. Implementation and supporting guidance should remain accessible and reasonable adjustments made where required.
Community / Public Impact	Low	Secure use of Council systems and effective asset management support continuity of services and protection of information held on behalf of residents and service users.
Procurement / Contractual	None	No procurement exercise or new contractual commitment is proposed through this report. Future equipment or service purchases remain subject to the Council's normal procurement and financial requirements.
Property / Asset	Medium	Asset management is a core part of the policy. Equipment must be tagged, recorded, protected, reviewed, returned and managed through defined loss, damage and replacement arrangements.
Data Protection	Medium	The policy requires secure handling of Council data, controlled use of devices and services, encrypted removable media where required, secure sharing and immediate reporting of suspected data breaches.

12. Appendices / Background Papers

12.1 Appendix A - ICT Acceptable Use and Asset Management Policy

12.2 Appendix B - Mobile Phone Staff Issue Form

12.3 Appendix C - PC, Laptop and Tablet Staff Issue Form

SALISBURY CITY COUNCIL

Appendix A ICT Acceptable Use and Asset Management Policy (Staff)

Policy Number	Version	Owner	Date Published	Review Date	Date Cllrs Review	Review Team
CORP/PO/006	1.0	IT Manager	September 2026	September 2027	October 2026	IT & HR

Distribution
Internal: All SCC Staff
External:

Contents

1. Introduction / Purpose

1.1 This policy sets out the acceptable use of ICT systems, devices, and services provided by Salisbury City Council (SCC).

1.2 This policy also sets out expected asset management of SCC issued ICT equipment and assets.

1.3 ICT provision is intended to support staff in delivering Council services effectively, securely, and in compliance with legal obligations.

1.4 This policy applies to all employees, contractors, agency staff, and third parties accessing SCC systems.

1.5 All users must read and comply with this policy and related information governance policies.

2. Policy Statement / Purpose

2.1 SCC ICT systems are provided primarily for business use.

2.2 Limited personal use is permitted provided it does not interfere with work duties, consume excessive resources, or breach policy.

2.3 Users must ensure their use of ICT complies with all relevant legislation including UK GDPR, Computer Misuse Act, Data Protection Act 2018 and Copyright law.

2.4 Users must not engage in activity that could harm SCC reputation, systems, or data.

3. Equipment and Devices

3.1 SCC may issue ICT equipment such as laptops or mobile devices to staff.

3.2 All equipment remains the property of the Council and must be returned upon request or termination of employment.

3.3 Users must take reasonable care of devices and prevent loss, theft, or damage.

3.4 Devices must not be used by unauthorised individuals.

3.5 Users must connect devices regularly to ensure updates and security patches are applied.

3.6 Users shall read the associated procedure document and sign the linked form on receipt of SCC issued ICT equipment and assets, which details that SCC (IT/Corporate) shall replace any lost, stolen or damaged asset on one occasion only. It is at the discretion of the IT Manager and Management Team as to how any subsequent losses are covered.

3.7 Users must report any failing or breaking equipment that may need to replaced to the IT Manager at the earliest opportunity.

4. Security and Data Protection

4.1 Protecting Council data is critical and all users must follow SCC Data Protection policies.

4.2 Sensitive and personal data must only be accessed where necessary and handled securely at all times.

4.3 Devices must be locked when unattended and used cautiously in public spaces.

4.4 Users must not store Council data on unapproved devices or services.

4.5 When required, users must use encrypted removable media, such as USB sticks. The use of non-encrypted removal media is not permitted.

5. Passwords and Authentication

5.1 Users must maintain strong passwords in line with SCC standards, namely:

- Passwords must contain at least three of the following categories:
  - Uppercase letters
  - Lowercase letters
  - Digits
  - Non-alphanumeric characters (!,$,# etc)

- Password cannot contain the user's account name pr parts of the user's display name.

- Passwords must be at least 7 characters long.

5.2 Passwords must never be shared.

5.3 Multi-factor authentication must be used where provided.

5.4 Accounts may be locked after repeated failed logon attempts.

5.5 Passwords must not be written down and left with equipment / taped to devices. MyGlue password manager (provided) must be used for all SCC password storage.

6. Software and Applications

6.1 Only approved software may be installed on SCC devices. Approved software list can be found in the procedure document entitled ‘Procedures & Guidelines for Salisbury City Council ICT Acceptable Use And Asset Management Policy (Staff)’.

6.2 Requests for additional software must be submitted to IT.

6.3 Users must not install unauthorised or unlicensed software.

6.4 IT reserves the right to remove unauthorised applications.

7. Connectivity and Remote Access

7.1 Users may access SCC systems remotely using the provided Azure VPN.

7.2 Public or unsecured networks must be used with caution.

7.3 Remote working must comply with SCC security standards.

7.4 Access to SCC systems must be from the UK. All other countries are blocked. Requests to allow temporary access from outside the UK must be requested to the IT Manager before arrival.

7.5 SCC staff who work from home will be issued a standard kit list for home desk setups.

8. Email and Microsoft 365 Use

8.1 SCC email accounts must be used for official communications.

8.2 Users must exercise caution when opening attachments or links to avoid phishing attacks.

8.3 Users must report suspicious communications using the provided security software.

8.4 Sensitive data must only be shared securely and with authorised recipients.

8.5 Council data must not be forwarded to personal email accounts.

8.6 Email signatures must follow the SCC format using Exclaimer unless exempt.

9. Mobile and Personal Devices

9.1 Users must read the Bring Your Own Device (BYOD) Policy to use personal devices for SCC work or on SCC networks.

10. Printing and Document Handling

10.1 Printing should be minimised wherever possible and should be in black and white. Colour printing should only be used when absolutely necessary.

10.2 Confidential information must be handled securely and disposed of appropriately.

10.3 Confidential documents should only be printed through 'Printix Anywhere' to protect data.

11. Incident Reporting

11.1 All security incidents must be reported immediately to the IT Manager and Corporate Services.

11.2 This includes lost devices, suspected breaches, or phishing emails via the provided software.

11.3 Data breaches must also be reported to the Data Protection Officer.

12. Care of, Lost, Theft or Damaged Equipment

12.1 SCC enforces a one-chance policy for PCs, laptops, tablets or any other kit issued to the user. If an employee loses, damages, or breaks a company-issued PC, laptop, tablet or other kit once, SCC may replace or repair the device without charge to the employee's department.

12.2 Any further incident involving loss, damage, or breakage will result in the full cost of repair or replacement being charged to the employee's department.

12.3 This applies regardless of whether the incident is accidental, unless an exception is approved by senior management.

12.4 Suspected data breaches must be reported immediately to the IT Manager and Corporate Manager and handled under SCC's Data Breach Procedure. Failure to report incidents promptly may result in disciplinary action.

12.5 All SCC issued assets must include asset tagging stickers with asset number. Asset will be logged in asset register under that number and associated with user.

12.6 Stickers must remain on all SCC issued assets. Should any sticker fade or become damaged, users must inform the IT manager so sticker can be replaced. This includes any host name identification sticker. EG: SCC-ABCDEF9

12.7 All assets will be looked after by the IT manager and stocked in a secure location.

12.8 A full stock check and review of equipment suitability will be carried out by the IT Manager annually.

13. Return of all equipment

13.1 All equipment must be returned upon termination of employment or upon request, in good condition, allowing for reasonable wear and tear, to the employee's line manager who must then return it to the IT Manager.

14. Monitoring

14.1 SCC may monitor use of ICT systems, including access logs, email, internet use and device activity where necessary and proportionate for security, compliance, audit investigation and service integrity purposes.

14.2 Monitoring is conducted to ensure security, compliance, and service integrity.

15. Roles and Responsibilities

15.1 Users are responsible for compliance with this policy.

15.2 IT Services will maintain and secure systems.

15.3 Managers must ensure staff are aware of and follow this policy.

15.4 Manages muse ensure staff leaver's issued assets are returned immediately to the IT Manager.

16. Associated Policies

16.1 E-Safety and Online Behaviours Policy

16.2 Bring Your Own Device (BYOD) Policy

16.3 Data Protection Policy

17. Review Procedure

17.1 This policy will be reviewed annually by IT Services and HR.

17.2 Approval will follow Council governance procedures, namely the Governance and Policy Committee.

Mobile Phone Acceptable Use Policy

Employee Acknowledgement Form

---

1. Purpose

This Mobile Phone Acceptable Use Policy (“Policy”) defines the acceptable use, care, and responsibility requirements for SCC-issued mobile phones. The purpose of this Policy is to protect company assets, ensure appropriate usage, and clarify employee accountability.

---

2. Scope

This Policy applies to all employees who are issued a company-owned mobile phone, including smartphones and any associated accessories (chargers, cases, SIM cards, etc.).

---

3. Ownership of Device

All mobile phones issued to employees remain the sole property of the Company. Issuance of a device does not transfer ownership rights to the employee.

---

4. Acceptable Use

Employees must:

- Use company-issued mobile phones primarily for business purposes
- Exercise reasonable care to prevent loss, theft, or damage
- Comply with all company policies, security requirements, and applicable laws
- Immediately report any loss, theft, or damage to their direct line manager

Limited personal use may be permitted provided it does not:

- Interfere with job performance
- Incur excessive costs
- Violate company policies or applicable laws

---

5. Prohibited Use

Employees must not:

- Use the device for illegal, unethical, or inappropriate activities
- Install unauthorized applications or modify device settings without approval
- Allow unauthorized individuals to use the device
- Disable security features installed by SCC

---

6. Device Care and Security

Employees are responsible for:

- Keeping the device secure at all times
- Using protective cases where provided
- Following security guidance, including PINs, passwords, or biometric controls
- Ensuring the device is not left unattended in public or unsecured locations

---

7. Loss, Theft, or Damage – One-Chance Policy

SCC operates a **one-chance policy** for company-issued mobile phones.

- If an employee **loses, damages, or breaks** a company-issued mobile phone **once in a calendar year**, SCC may replace the device at no charge to the employee's department.
- **Any subsequent loss, damage, or breakage**, whether accidental or due to negligence, **will result in the cost of replacement or repair being charged to the employee's department or written off with no departmental charge at the IT Manager's discretion**.
- This applies regardless of the circumstances, except where otherwise determined by senior management.

Failure to promptly report loss or damage may be treated as misconduct.

---

8. Return of Device

Upon termination of employment or upon request, the employee must return the mobile phone and all accessories in good working condition, allowing for reasonable wear and tear.

---

9. Policy Violations

Violation of this Policy may result in:

- Withdrawal of mobile phone privileges
- Disciplinary action

---

10. Employee Acknowledgement

I acknowledge that I have read, understood, and agree to comply with the Mobile Phone Acceptable Use Policy. I understand my responsibilities and the consequences of failing to adhere to this Policy.

Employee Name: _____

Employee Signature: _____

Department: _____

Date: _____

PC, Laptop and Tablet Acceptable Use Policy

Employee Acknowledgement Form

---

1. Purpose

This PC, Laptop and Tablet Acceptable Use Policy (“Policy”) establishes requirements for the proper use, care, and protection of company-issued computing devices. The Policy aims to safeguard company information, systems, and assets.

---

2. Scope

This Policy applies to all employees who are issued a company-owned PC, laptop, or tablet, including all peripherals and accessories.

---

3. Ownership of Equipment

All PCs, laptops, and tablets issued to employees remain the exclusive property of the Company. Employees are granted permission to use these devices solely in accordance with this Policy.

---

4. Acceptable Use

Employees must:

- Use company-issued devices primarily for business purposes
- Protect company data and comply with information security requirements
- Lock devices when unattended and store them securely
- Promptly report any loss, theft, or damage to their direct manager

Limited personal use may be permitted provided it does not:

- Compromise security
- Violate company policies or applicable laws
- Interfere with work responsibilities

---

5. Prohibited Use

Employees must not:

- Install unauthorized software or hardware
- Disable antivirus, encryption, or security controls
- Use devices for unlawful, unethical, or inappropriate activities
- Share devices with unauthorized individuals

---

6. Device Care and Security

Employees are responsible for:

- Taking reasonable steps to prevent loss, theft, or damage
- Transporting devices safely, including during travel
- Keeping devices protected from physical and environmental damage
- Following all IT security and data protection guidelines

---

7. Loss, Theft, or Damage – One-Chance Policy

SCC enforces a **one-chance policy** for PCs, laptops, and tablets.

- If an employee **loses, damages, or breaks** a company-issued PC, laptop, or tablet **once**, SCC may replace or repair the device without charge to the employee's department.
- **Any further incident involving loss, damage, or breakage** will result in the **full cost of repair or replacement being charged to the employee's department or written off with no charge at the IT Manager's discretion**.
- This applies regardless of whether the incident is accidental, unless an exception is approved by senior management.

Failure to report incidents promptly may result in disciplinary action.

---

8. Return of Equipment

All equipment must be returned upon termination of employment or upon request, in good condition, allowing for reasonable wear and tear.

---

9. Policy Violations

Non-compliance with this Policy may result in:

- Removal of device access
- Disciplinary action

---

10. Employee Acknowledgement

I confirm that I have read, understood, and agree to comply with the PC, Laptop and Tablet Acceptable Use Policy. I understand my responsibilities, including the one-chance policy for loss or damage.

Employee Name: _____

Employee Signature: _____

Department: _____

Date: _____