# COMMITTEE REPORT

| | |
|---|---|
| ***Subject:*** | *E-safety and Online Behaviours Policy* |
| ***Committee:*** | *Governance, Policy & HR Committee* |
| ***Item Number:*** | *11* |
| ***Date:*** | *5 October 2026* |
| ***Author:*** | *Jeremy Cotton, IT Manager* |
| ***Report status:*** | *Decision* |
| ***Confidential / Exempt:*** | *No* |

## 1. Report Summary

This report asks the Committee to consider the Salisbury City Council new E-safety and Online Behaviours Policy for members and officers. The policy establishes mandatory online safety behaviours for staff and sets out controls for phishing, social engineering, malware, unsafe content, internet and email use, social media, online data protection, and remote and mobile working.

The purpose of this report is to ask Committee approval of the E-safety and Online Behaviours Policy at Appendix A.

1.1 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.

1.2 The policy is intended to reduce cyber incidents caused by human error or manipulation, help staff recognise and respond to common online threats, protect SCC systems and data, protect the Council's reputation, and protect staff and members from online harm.

1.3 The policy is being brought forward to provide a specific framework for safe online behaviour and threat awareness, complementing the ICT Acceptable Use and Asset Management Policy.

1.4 The recommended course of action is to recommend adoption of the E-safety and Online Behaviours Policy through the Council's governance procedures.

## 2. Recommendations

It is recommended that the Committee:

2.1 To approve the E-safety and Online Behaviours Policy at Appendix A.

## 3. Background

3.1 The policy recognises that staff and SCC systems are exposed to phishing, social engineering, malware, ransomware, account compromise, harmful websites, data leakage, impersonation and fraud. It states that online threats continue to evolve in sophistication and frequency and can target individuals and organisations through email, web browsing and digital collaboration platforms.

3.2 The policy is owned by IT Service, has a stated version of 1.0. The policy states that approval will follow Council's governance procedures.

3.3 The policy complements the ICT Acceptable Use and Asset Management Policy. It addresses risk prevention, safe behaviours and threat awareness, and includes requirements concerning data protection, remote working, social media, email and internet use, mandatory IT training and incident reporting.

## 4. Proposal

4.1 The proposal is to adopt the new E-safety and Online Behaviours Policy, found in Appendix A, as the Council's framework for mandatory safe online behaviour and cyber-security awareness for staff.

4.2 The proposal provides a clear and consolidated set of behaviours covering verification of emails and requests, phishing and social engineering, malware and ransomware, internet and email safety, social media, online data protection, and remote and mobile safety.

4.3 The intended outcomes are reduced exposure to cyber incidents arising from human error or manipulation; improved recognition and reporting of phishing and other suspicious activity; better protection of SCC systems and data; safer handling of personal and sensitive information; and increased awareness of online risks among staff.

4.4 Action is required to establish and communicate the expected behaviours and reporting requirements set out in the policy and to support the Council's wider information security and data protection arrangements.

## 5. Financial Position

5.1 The policy does not specify a new financial cost, budget allocation or funding requirement. It does, however, require SCC to support the policy through training, awareness campaigns, simulated phishing exercises and timely alerts, which will require existing staff and IT resources.

5.2 No specific external funding, grant or new budget provision is identified in the policy. Any additional expenditure arising from implementation would need to be considered through the Council's normal budget and approval processes.

5.3 There will be ongoing staff and IT resource requirements associated with mandatory IT training, awareness campaigns, simulated phishing exercises and responding to online security incidents. The policy does not quantify these costs.

5.4 There will be ongoing resource requirements associated with members' mandatory IT training, awareness campaigns, simulated phishing exercises and responding to online security incidents. The policy does not quantify these costs but this is covered by members training budget.

## 6. Legal and Governance Considerations

6.1 The policy itself does not identify a specific statutory power for adoption. The legal basis and authority for the decision should be confirmed through the Council's governance and approval process before publication.

6.2 The policy requires users to comply with data protection requirements when handling personal or sensitive information and establishes controls for secure data transfer, authorised recipients, access permissions and reporting suspected data breaches. The policy also states that approval will follow Council governance procedures.

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.

## 7. Consultation and Engagement

7.1 The policy document contains internal comments concerning its scope and wording, including confirmation that it complements the ICT Acceptable Use and Asset Management Policy, clarification that there is no separate social media policy, and comments concerning safe disconnection from networks and public Wi-Fi. No wider public or resident consultation is identified in the policy.

7.2 The policy's documented requirements focus on mandatory user behaviours, reporting of suspicious activity, secure handling of data, remote and mobile safety, and staff awareness and training.

7.3 No formal resident or public consultation is identified in the policy. The subject is primarily an internal staff cyber-security and information governance control.

7.4 Follow up with staff and member awareness of the policy with relevant training and phishing exercises.

## 8. Strategic and Policy Alignment

8.1 The policy supports the Council's operational need to protect its systems, information, staff and reputation from online harm. It provides a framework for risk prevention, safe behaviours and threat awareness and supports responsible use of online services.

8.2 The policy complements the ICT Acceptable Use and Asset Management Policy (Staff) and includes requirements relevant to data protection, cyber security, remote working and the use of online services.

## 9. Implementation and Next Steps

9.1 Subject to the Committee's decision, the next steps will be as follows:

9.1.1 Complete the required governance and approval checks for the policy.

9.1.2 Communicate the policy and mandatory online safety requirements to SCC staff and incorporate the requirements into relevant IT awareness and training activity.

9.1.3 Implement and maintain the supporting awareness measures, including training, simulated phishing exercises and alerts about emerging threats for both officers and members.

9.1.4 Review the new policy in accordance with the Policy and Procedure Management

Policy.

9.2 Responsibility for implementation will sit with IT Service, working with HR and relevant managers through the Council's governance arrangements.

## 10. Additional Relevant Information

10.1 No additional information is required beyond the matters set out above and the policy itself.

10.2 The report is intended to provide the information required for an informed governance decision, with the policy forming the substantive document for adoption.

## 11. Implications

| Implication Area | Impact | Comments / Mitigation |
|---|---|---|
| **Financial** | Low | No specific new cost is identified in the policy. Training, awareness, simulated phishing and incident response will require IT/HR resources; any additional expenditure should be considered through normal budget processes. |
| **Legal** | Medium | The policy contains requirements relating to data protection and online conduct, but does not state the specific legal power for adoption. Legal/governance confirmation should be completed before approval. |
| **Risk** | Medium | The policy addresses phishing, social engineering, malware, ransomware, account compromise, data leakage and other online threats. Mitigation is through mandatory behaviours, reporting, training, awareness and secure data handling. |
| **Personnel** | Low | All users must complete mandatory IT training. Staff will also be expected to follow the specified online safety behaviours and report suspicious activity. |
| **Environmental Impact** | None | The policy does not identify a material environmental impact. |
| **Equalities Impact Statement** | Low | No specific adverse equality impact is identified in the policy. The requirements apply to all SCC staff and should be implemented in a manner consistent with applicable equality duties. |
| **Community / Public Impact** | Low | The policy is an internal staff control, but improved online safety supports protection of Council services, information and the public information handled by SCC. |
| **Procurement / Contractual** | Low | The policy does not require a specific procurement exercise. Any future purchase of training, security or online services would be subject to the Council's normal procurement and financial requirements. |
| **Property / Asset** | None | The policy does not identify a material impact on Council buildings, land or physical assets. |
| **Data Protection** | Medium | The policy requires secure transfer of SCC data, authorised recipients, restricted sharing permissions, protection of sensitive information and immediate reporting of suspected data breaches or incorrect disclosures. |

## 12. Appendices / Background Papers

12.1 Appendix A – E-safety and Online Behaviours Policy

SALISBURY CITY COUNCIL

# Appendix A
# E-Safety and Online Behaviours Policy

| Policy Number | Version | Owner | Date Published | Review Date | Review Team |
|---|---|---|---|---|---|
| CORP/PO/007 | 1.0 | IT Manager | September 2026 | September 2027 | IT & HR |

**Distribution**
**Internal**: All SCC Staff
**External**: Website

**Contents**

## 1. Introduction

1.1 Salisbury City Council (SCC) recognises that staff and systems are exposed to a wide range of online safety threats, including phishing, social engineering, malware, ransomware, account compromise, harmful websites, data leakage, and impersonation or fraud.

1.2 Threats continue to evolve in sophistication and frequency, targeting both individuals and organisations through email, web browsing, and digital collaboration platforms. This policy defines how SCC mitigates these risks by promoting safe behaviours, threat awareness, and responsible use of online services.

1.3 The purpose of this policy is to:

- Reduce the likelihood of cyber incidents caused by human error or manipulation
- Ensure staff can recognise and respond to common online threats
- Protect SCC systems, data, and reputation from online harm
- Protect SCC staff from online harm

1.4 This policy complements the Acceptable Use and Asset Management Policy (Staff) and focuses specifically on:

- Risk prevention
- Safe behaviours
- Threat awareness.

## 2. Mandatory User Behaviour

2.1 All users must follow the following core safety principles:

2.1.1 Users must verify the legitimacy of emails, links, and requests before taking action

2.1.2 Users must only use approved and trusted services for file sharing and communication

2.1.3 Users must check sender details carefully before responding to or acting on email communications

2.1.4 Users must exercise caution when handling unexpected requests, particularly those involving money, credentials, or sensitive information

2.1.5 Users must not open attachments from unknown, untrusted, or unexpected sources

2.1.6 Users must not provide passwords, authentication codes, or sensitive information via email or unverified communication channels

2.1.7 Users must use unique passwords for SCC systems and must not reuse these passwords across personal accounts

## 3. Phishing and Social Engineering

3.1 Users must treat all unsolicited or unexpected communications as potentially malicious.

3.2 Users must verify the identity of the sender before responding to any request for information, access, or financial action.

3.3 Users must not act on requests that attempt to bypass established processes or controls.

3.4 Users must not click on links or open attachments unless they are confident of the source and legitimacy.

3.5 Using SCC-approved reporting tools, users must immediately report:

3.5.1 Any suspected phishing email or message

3.5.2 Any request for sensitive information that appears unusual or suspicious

3.5.3 Any communication that uses urgency, pressure, or authority to influence behaviour

3.6 Users must not:

- Respond to, engage with, or forward suspected phishing emails
- Provide passwords, authentication codes, or sensitive information in response to email or messaging requests
- Attempt to test or interact with suspicious content beyond what is required to report it

## 4. Malware, Ransomware and Unsafe Content

4.1 Users must not download or run files unless they are confident of their legitimacy.

4.2 Users must immediately report antivirus or security alerts, locked files / ransom messages or other unusual system behaviours to the IT Manager. Users must disconnect devices from the network if safe to do so.

4.3 Users should disconnect the device from the network if any suspicious behaviour is observed.

## 5. Internet and Email Safety

5.1 Internet usage must be conducted safely, responsibly, and in a manner that protects SCC, its staff, and the public.

5.2 Users must:

5.2.1 Access only trusted and work-appropriate websites

5.2.2 Be cautious of websites requesting downloads or personal information

5.2.3 Check website addresses (URLs) for legitimacy before entering credentials

5.3 Users must not:

5.3.1 Attempt to access, download, or upload material that is obscene, sexually explicit, racist, defamatory, or which incites or depicts violence

5.3.2 Access content intended to cause distress or that describes techniques for criminal or terrorist activity

5.3.3 Intentionally access, introduce, or transmit malware, viruses, or harmful code

5.3.4 Attempt to bypass security controls or ‘hack’ systems, websites, or data

5.3.5 Use loopholes in systems or websites to access, alter, or damage data

5.3.6 Infringe copyright, including unauthorised downloading or sharing of images, apps, games, music, or other content

5.3.7 Use SCC systems for gambling or access payday loan or similar high-risk financial websites

5.3.8 Undertake any online activity that could bring SCC into disrepute

5.4 SCC may restrict or block access to certain categories of websites to reduce risk.

5.5 Email presents a significant cyber risk and must be used carefully and responsibly.

5.6 Users must:

5.6.1 Verify sender identity before acting on requests

5.6.2 Treat unexpected attachments or links with caution

5.6.3 Double-check recipient addresses before sending emails

5.6.4 Comply with data protection requirements when sending personal or sensitive information

5.7 Users must not:

5.7.1 Send, receive, or distribute material that is offensive, abusive, violent, obscene, racist, or defamatory

5.7.2 Send content that could be considered harassment, including inappropriate jokes or images

5.7.3 Use email for unsolicited advertising or private commercial activity

5.7.4 Flood the network with unnecessary emails or large attachments that could disrupt services

5.7.5 Send information that could bring SCC into disrepute

5.8 Users should take care not to:

5.8.1 Share personal details unnecessarily via email

5.8.2 Arrange meetings or share sensitive information with unknown individuals

## 6. Social Media and Online Communication

6.1 Access to social media platforms may be restricted unless approved for business purposes.

6.2 Where access is permitted, users must:

6.2.1 Use social media safely and professionally

6.2.2 Avoid sharing personal or sensitive information

6.2.3 Ensure appropriate privacy and security settings are applied

6.2.4 Only interact with known or trusted individuals online

6.2.5 Immediately report any suspicious or concerning online behaviour to their line manager

## 7. Data Protection Online

7.1 Users must only transfer SCC data using approved and secure methods, including:

7.1.1 SCC email systems (with appropriate protections applied)

7.1.2 Approved cloud storage platforms (e.g. M365 / SharePoint / OneDrive)

7.1.3 Secure file transfer solutions provided by SCC

7.2 Users must not use:

7.2.1 Personal email accounts

7.2.2 Unapproved cloud storage or file-sharing services

7.2.3 Public file transfer websites or tools

7.3 Users must apply appropriate protection when transferring data, including:

7.3.1 Encrypting sensitive or personal data where required

7.3.2 Using password protection for documents containing confidential information

7.3.3 Sharing links with restricted access permissions (named users only where possible)

7.4 Users must verify:

7.4.1 The identity of recipients

7.4.2 That recipients are authorised to receive the data

7.5 Users must not:

7.5.1 Send data to incorrect or unverified recipients

7.5.2 Share sensitive or personal data via insecure methods

7.5.3 Upload SCC data to unauthorised systems or platforms

7.5.4 Store SCC data on personal devices or removable media without approval

7.6 When using file sharing platforms, users must:

7.6.1 Set appropriate access permissions (e.g. “view only”)

7.6.2 Remove access when no longer required

7.6.3 Avoid “anyone with the link” sharing unless explicitly approved

7.7 Users must immediately report any suspected data breach, loss or unauthorised access to data or data sent to the wrong recipient to the data protection officer.

## 8. Remote and Mobile Safety

8.1 Users should avoid public Wi-Fi where possible and must use approved secure access methods where remote access is required.

8.2 Users must be aware of screen visibility in public places and lock screens where appropriate.

8.3 Users must keep devices physically secure at all times and must not leave SCC devices unattended.

## 9. Awareness and Responsibility

9.1 Cyber security is a shared responsibility. Users must complete all mandatory IT training courses provided.

9.2 SCC will support this through:

9.2.1 Regular training and awareness campaigns

9.2.2 Simulated phishing exercises

9.2.3 Timely alerts about emerging threats

## 10. Review Procedure

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

10.2 Approval will follow Council governance procedures.