WILTSHIRE COUNCIL **AGENDA ITEM NO.**

Staffing Policy Committee
DATE 8th November

Acceptable Use Policy

Purpose

1. The purpose of the report is to update SPC on changes which need to be made to the Acceptable Use Policy, including the introduction of Multi-Factor Authentication (MFA).

Background

2. The Acceptable Usage Policy was last updated in 2021.

3. This policy needs to be reviewed regularly to ensure that the council continues to employ the most robust security tools available, to prevent successful cyberattacks.

4. The changes made in this version of the policy – most notably the introduction of MFA – are designed to not only help Wiltshire Council comply with data protection laws, and the expectations set by Central Government around how Local Authorities should meet their Cyber Security aims, but also to embed good cyber security practices, which will improve our overall cyber security resilience.

5. There are also growing expectations from third party suppliers and partners, that MFA will be a requirement of gaining access to their information and systems.

Main considerations

6. Multi Factor Authentication (outlined in section 11.1 of the policy).

   6.1. MFA confirms a person is who they say they are by using more than one authentication method. Something they know (a password) as well as something they have (another device) or something they are (biometrics) this way if a password is compromised, they would still need access to another form of authentication to gain access.

   6.2 To set MFA, employees have the option (in addition to their existing password) to pick one or more of the following methods:

   - App-based authentication (Preferred) – Download an authentication app onto their mobile device.

- SMS-based authentication – Request an SMS text message to a mobile device
- Phone Call (landline and mobile) – Request a phone call to a number without an auto attendant, such as a direct dial or landline number.

6.3 If all the above methods are not suitable to the employee, then they should speak with their line manager and an authorisation token can be purchased and charged to the service.

6.4 MFA will launch to employees in October 2023, and the first cloud application that will utilise this will be Oracle, launching under the programme Evolve in November 2023.

7. The introduction of a Secure Email section within the policy (section 6.1 of the attached policy) will make employees aware of how this provision has changed, and what they need to do to check if secure email has been setup for the external company they are working with. This means that ICT have carried out checks on the email address or domain, before setting up a secure email connection to send personal or special category information. This helps the council be compliant with data protection legislation.

8. The introduction of a Phishing and Spear-Phishing section (section 6.2 of the attached policy) to provide up to date information on what to do and what not to do if you receive a suspicious email. This supersedes previous advice relating to use of Mimecheck.

9. The addition of an ID badges section (section 10 of the attached policy) to highlight when to wear and when to remove Wiltshire Council ID badges to raise awareness of the security risks presented when ID badges are worn outside of council sites.

10. There have also been some minor wording improvements to make other sections of the policy easier to read, or to reflect changes in how services can be accessed – however these do not make any significant changes to the content, or the expected behaviours.

Reason for the policy/ changes to the policy

11. Changes have been made to the policy to reflect increasing need for measures such as MFA, and to provide updated information about phishing and spear phishing.

Environmental impact of the proposal

12. Potential environment implications of rolling out MFA, where colleagues do not opt to use the default MFA provision.

Equalities impact of the proposal

13. No impact. AUP assessed at the Equalities Analysis Panel on 12th October.

Risk Assessment

14. In relation to MFA - Employees may not want or have a suitable means to add an authentication app to their personal device and in this instance they can either select to receive an SMS text message or request a callback to a mobile or landline number. Again, if this step is not acceptable then an authentication token can be purchased and cross charged to the service.

Financial Implications of the proposal

15. Potential financial implications of rolling out MFA, where colleagues are not able/prepared to use the default MFA provision. In this case token cost will be charged to the appropriate service area.

Recommendations

16. It is recommended that SPC approve the Acceptable Use Policy.

Tamsin Kielb
Director HR&OD

Report Author: Sarah Davis-Solan, Information Assurance & Monitoring Lead