TEWKESBURY BOROUGH COUNCIL

Report to:	Executive Committee
Date of Meeting:	6 September 2023
Subject:	ICT Acceptable Use Policy
Report of:	Associate Director: IT and Cyber
Head of Service/Director:	Executive Director: Resources
Lead Member:	Lead Member for Corporate Governance
Number of Appendices:	One

Executive Summary:

The existing ICT Acceptable Use Policy was approved in April 2019 prior to the pandemic. Since that time, the Council has made significant changes to its flexible working, the software it uses and the technology that is issued. During this time, the cyber security risk to the council has changed and become more complex to manage. As such it is good practice to review the acceptable use policy to ensure it is fit for purpose and make any amends necessary to ensure the council can deliver its ICT in a safe and sustainable way.

Recommendation:

1. **To APPROVE the revised ICT Acceptable Use Policy which will require all Officers and Members to sign a declaration of acceptance to ensure full compliance.**
2. **To DELEGATE AUTHORITY to the Associate Director: IT and Cyber, in consultation with the Lead Member for Corporate Governance, to make minor changes to the policy including changes to management structure, typographical changes etc.**

Financial Implications:

The policy restricts access to Council data to Council-owned devices. As such, there is a need to issue a small number of additional mobile phone to Officers who are currently using their own phones for work purposes. The costs of this are approx. £4,000; these costs can be met from existing ICT budgets and reserves.

Legal Implications:

The ICT Acceptable Use Policy clearly sets out the responsibilities and obligations of users of the Council's ICT resources including their legal obligations. All ICT users will be required to confirm their acceptance of the ICT Acceptable Use Policy by signing a declaration of acceptance. This will enable the Council to take appropriate action for breaches of policy.

Environmental and Sustainability Implications:

None

Resource Implications (including impact on equalities): None
Safeguarding Implications: None
Impact on the Customer: The revised policies improve the security of the Council and help protect it from attackers who might wish to disrupt the Council's services.

1.0 INTRODUCTION

1.1 The safe and appropriate use of technology is critical to ensuring the Council can deliver services while minimising the risks caused by the either accidental or deliberate misuse of software, computers and mobile devices.

1.2 The revised ICT Acceptable Use Policy reflects changes in ICT that have occurred since the last policy was approved in 2019, addresses the rise in cyber threats facing the Council and reflects new ways of working the Council has adopted.

2.0 CHANGES TO ACCEPTABLE USE POLICY

2.1 The revised policy includes the following changes:

- Only authorised equipment issued by the Council can be used to carry out Council business. Users must not use any unapproved equipment to access data or carry out Council business. This includes personal mobile phones, tablets, computers and laptops.
- A requirement to report any incidents of suspected or actual security breaches, violations of policies or procedures, or any other concerns related to the use of ICT services to the IT department immediately.
- All Council resources, including but not limited to computers, mobile devices, software, and internet access, are provided for business purposes only. It is the responsibility of all users to use Council resources solely for work-related activities and refrain from using them for personal activities, such as browsing social media, personal email, online shopping, personal business, political activities, or any other non-work-related activities.
- By default, access to ICT services and Council data (including accessing Office 365, email or Teams) is restricted to locations within the UK. Systems that bypass location detection or content control systems such as VPNs and proxies are not permitted to be used with Council equipment or data unless specifically authorised by the IT department.
- Access to email and Teams will be granted to users travelling within the EU on their corporate mobile devices (phones and tablets). The devices must be kept securely locked away and it is expected they will be used in a safe way (e.g. not in the middle of the street). This access will not be enabled by default and will need to be requested in advance to balance the security of the organisation while offering additional flexibility to respond to urgent incidents.

- To ensure the security of communication, only email addresses issued by the Council can be used for official Council business. Personal email accounts must not be used for any Council-related activities. Using personal email accounts may compromise the security and confidentiality of Council information and could violate Council policies and procedures.

3.0 CONSULTATION

3.1 Consultation on the policy documents has been undertaken with One Legal and the Council's Leadership Team.

4.0 ASSOCIATED RISKS

4.1 Misuse of ICT poses a significant risk to the Council. Failure to use ICT in accordance with the policy will significantly increase the Council's data protection risks, the risks of cyber attack and the risks of malicious activity. Each of these risks could pose a significant reputational and financial impact to the Council.

5.0 MONITORING

5.1 Policy will be monitored according to the procedures documented in the policy and in accordance with any relevant legislation.

6.0 RELEVANT COUNCIL PLAN PRIORITIES/COUNCIL POLICIES/STRATEGIES

6.1 None

Background Papers: ICT Acceptable Use Policy

Contact Officer: Associate Director: IT and Cyber
01684 272158 Iain.Stark@tewkesbury.gov.uk

Appendices: Appendix 1 – Revised ICT Acceptable Use Policy