# Surrey Heath Borough Council
# Employment Committee
# 28th March 2024

---

## Email Security Policy

| | |
|---|---|
| **Strategic Director/Head of Service** | Gavin Ramtohal |
| **Report Author:** | Sally Turnbull - Information Governance Manager |
| **Key Decision:** | No |
| **Wards Affected:** | n/a |

---

### Summary and purpose

This report provides details of the Email Security Policy. This is a new policy and being brought to the Employment Committee for approval.

### Recommendation

The Committee is advised to RESOLVE that the Email Security Policy as set out at Annex A to this report, be adopted.

### 1. Background and Supporting Information

1.1 The Council must ensure the security of its information and its network, one of the biggest risks to this is email and the email users use of email.

1.2 ICT are putting in place controls to protect the Council against improper sharing of information and cyber-attack via email, email users need to be aware that these controls are in place and understand why and how they are being used by the Council.

1.3 Email security is currently covered in the Information Security (IS) Policy however this is more top level and is spread out across the very large IS policy. The new Email Security Policy is a much more focussed and detailed policy, that will work alongside the IS Policy.

1.4 This policy was reviewed by the Joint Staff Consultative Group on 7th March 2024 and has been amended with the Group's comments accordingly.

### 2. Reasons for Recommendation

2.1 The Email Security Policy sets out the framework for compliance with the requirements of the Councils Information Security Policy and Data Protection Legislation. It provides Council email users with an understanding of how email should be managed and is being monitored by the Council. It provides guidance to all Council email users to help them understand the correct and safe use of email.

2.2 With the rollout of the Data Loss Shield alerts being activated on all email users outlook, a reference point is required to link to within the alerts so users can understand why they are receiving alerts and have a clear understanding of what the Councils policy is on email security.

## 3. Proposal and Alternative Options

3.1 It is proposed that the policy is adopted, with or without any further amendments considered appropriate.

## 4. Contribution to the Council's Five Year Strategy

4.1 No matters arising.

## 5. Resource Implications

5.1 There are no additional revenue or capital cost implications arising from the policy.

## 6. Section 151 Officer Comments:

6.1 This policy has gone through CMT whereby the Section 151 Officer provided comment which has been fed into the policy.

## 7. Legal and Governance Issues

7.1 The Council has a legal obligation under GDPR to ensure the security of its information, the policy aims to educate and inform staff on the correct and safe use of email. The policy also aims to achieve transparency to staff around how the Council monitors and secures email.

## 8. Monitoring Officer Comments:

8.1 This policy has gone through CMT whereby the Monitoring Officer provided comment which was fed into the policy.

## 9. Other Considerations and Impacts

### Environment and Climate Change

9.1 n/a

### Equalities and Human Rights

9.2 Equalities Impact Assessment will be completed.

### Risk Management

9.3 Information Management and Security is identified as a Corporate risk on the risk register, a Email Security Policy could assist with mitigating the risk further.

### Community Engagement

9.4 n/a

### Annexes

Annex A - Email Security Policy