RMCC Best Practices for Email Management in Council Communications Notes Guide (Draft)

Introduction

This document outlines the best practices for managing email communications within council operations. It highlights the importance of using official council email addresses, the risks associated with using personal email accounts for council business, and provides guidelines to ensure legal compliance.

1. Importance of Using a Council-Specific Email Address

Professionalism

A dedicated council email address ensures that all communications are professional and clearly associated with the council.

Example: Emails sent from 'clerk@councilname.gov.uk' appear more official and credible than those sent from a personal address like 'john.smith@gmail.com.'

Accessibility

Using a council-specific email address ensures that the public can easily contact the council.

Legal Reference: As per the Local Government (Democracy) (Wales) Act 2013, councils must publish their contact details electronically, including an email address.

Example: 'info@councilname.gov.uk' should be published on the council's website for public inquiries.

2. Risks of Using Personal Email Accounts

Security Risks

Personal email accounts may not have the same security measures as official council accounts, increasing the risk of data breaches.

Legal Implication: Councillors are subject to the Data Protection Act 2018, which requires secure handling of personal data.

Example: A councillor using 'john.smith@gmail.com' risks exposure of confidential council information if their personal email account is compromised.

Legal Risks

Using personal emails for council business can blur the line between personal and official communications, complicating legal responsibilities under the Freedom of Information Act 2000 (FOI).

Example: If a FOI request is made, all relevant council communications, including those in personal email accounts, must be disclosed, potentially exposing private information.

Accountability and Record Keeping

Official emails must be retained as part of council records. Personal accounts may not have adequate archiving systems, leading to the potential loss of important information.

Legal Reference: Councils are required to maintain records for transparency and accountability.

Example: 'clerk@councilname.gov.uk' ensures that all communications are archived and accessible for legal or audit purposes, unlike a personal account.

Risks Related to Subject Access Requests (SARs)

Under the Data Protection Act 2018, individuals have the right to request access to personal data held about them, known as a Subject Access Request (SAR). Using personal email accounts for council business increases the complexity and risk of failing to comply with SARs.

Legal Implication: Councillors are data controllers in their own right, and failure to properly respond to a SAR can result in legal penalties.

Example: If a personal email account is used for council business and a SAR is made, all emails containing personal data related to the request must be searched and disclosed. This can be difficult if personal and council communications are mixed, leading to potential non-compliance with SAR requirements.

3. Best Practices for Email Management

Creating a Dedicated Email Account for Council Business

Recommendation: Each council member and official should have a council-specific email address (e.g., 'firstname.lastname@councilname.gov.uk').

Example: The Chair could have 'chair@councilname.gov.uk' for all official correspondence.

Regular Monitoring and Response

Recommendation: Set a schedule to check and respond to emails regularly.

Example: Daily checks to ensure no critical communications are missed.

Archiving and Record-Keeping

Recommendation: Use email management tools that archive all communications for future reference and legal compliance.

Example: Implementing an email archiving solution that automatically saves all emails sent and received to a secure, searchable database.

Security Measures

Recommendation: Enable multi-factor authentication (MFA) on all council email accounts to protect against unauthorized access.

Example: Requiring a verification code in addition to a password for login.

4. Legal Requirements and Compliance

Data Protection Act 2018

Councillors must ensure that personal data is handled securely, which is more reliably done through official council accounts.

Example: Avoiding the use of personal accounts minimizes the risk of unintentional data breaches.

Freedom of Information Act 2000

All council-related communications are subject to FOI requests, and using personal email accounts can complicate the retrieval of these communications.

Example: An official email system ensures that all relevant communications can be easily accessed and provided if requested.

Subject Access Requests (SARs)

SARs require councils to provide individuals with access to personal data held about them. Using personal email accounts for council business increases the risk of failing to locate and disclose all relevant information.

Example: An official email account allows for easier compliance with SARs by centralizing all council-related communications, reducing the risk of missing relevant data.

5. Conclusion

Using official email accounts for council business is critical for professionalism, security, and legal compliance. By following the best practices outlined above, councils can mitigate risks and ensure they meet all legal requirements.

References

Module 16 - Use of IT, Websites & Social Media Training Booklet 2024.

Local Government (Democracy) (Wales) Act 2013.

Data Protection Act 2018.

Freedom of Information Act 2000.