Un Llais Cymru
One Voice Wales

Community & Town Councils Digital Guidance

Use of Email

November 2024

Contents

Introduction

This guidance document is intended to help Community and Town Councils in Wales understand and consider issues around provision and use of email for conducting council business and interacting with the public.

It should be read in conjunction with related guidance around Domain Names and Websites

All Community and Town Councils in Wales should adopt good email practices. This will allow councils to benefit from the efficiency and convenience associated with electronic communication while managing risks associated with security and privacy breaches.

Requirements

There are no specific legislative or regulatory requirements guiding the detail of how Community and Town Councils use emails – other than providing a means to contact the Council on the website. However, there are key considerations of which Councils should be aware when choosing their approach.

Compliance

Councils need to maintain proper records of communications and emails should be managed in the same way as other written communications. Email correspondence should be stored, archived and disposed of according to Council policy.

Approach

Personal Emails

Many councillors and some staff continue to use personal email accounts (i.e. accounts which they also use to conduct their personal affairs) for Council business. There are several risks associated with using personal email addresses which makes this an unacceptable approach. These risks also apply to the use of an employer's email address or another Council's address for Council purposes.

Risks of Using Personal Email Addresses:

Subject to Impersonation: Personal email addresses can often be easily impersonated by simple techniques such as changing a single character as well as spoofing where someone alters an email to give the impression it has been sent by someone else.
Security: Personal email accounts may have weaker security protocols deployed compared to those offered by professional email providers. This increases the risk of data breaches and unauthorized access to sensitive council information.
Continuity: When a councillor leaves their position, important Council emails might be lost if they were sent to a personal account. This can disrupt communication and hinder future reference.
Transparency: Public access to Council information requests may become complicated if official communication is scattered across personal email accounts.
Accountability: Personal email use can make it difficult to track communication and ensure proper record-keeping for Council activities.
Freedom of Information Requests: Communications concerning Council business can be subject to Freedom of Information requests and it is difficult and disruptive if councillors need to disclose personal emails as part of e.g. a subject access request asking for all references to an individual in council emails.
Reputational Risk: Having a light-hearted or comical personal email address may be fine for friends and families but is unlikely to reflect well on the Council.

Best Approach for Council Email Services:

Choosing the best approach for Council email services will involve some trade-offs between functionality, administrative overhead and costs.

The approaches are the same for services for staff and Councillors but provision of service for staff must be a priority.

Option 1: Council Provided Email Services:

The council can purchase an email service for staff (and for councillors). This can be as part of a broader "collaboration" package (such as Microsoft 365 or Google Workspace), or it can be a simple email address and mailbox. There will be a cost for this which will depend on the service which is purchased. Some website providers will supply basic email services as a free or low-cost extra to their website hosting services
This level should be strongly considered for any office-based staff such as clerks
Pros: Provides individual email addresses for staff and councillors, fosters professionalism, improves communication flow.
Cons: Requires initial setup and ongoing maintenance, may incur a cost depending on the chosen provider, needs staff and councillors to monitor and manage their emails.

Option 2: "Free" Email Services (e.g. Gmail, Outlook, Yahoo etc):

Councillors can create a free to use (advertising supported) email service which can be kept separate from any email or other online accounts which they use for personal business.

Pros: Often free or low-cost, familiar interface for many users, usually bundled with other features (calendars, file storage). Facilitates responding to any Freedom of Information, subject access request or other request for council information as there is no need to redact councillor's personal, non-council, information
Cons: A specific policy will need to be put in place to define how the council manages these email accounts e.g. if a councillor steps down what happens to their email account? A free account will have advertising which will be a potential distraction from council business. Free to use accounts may not provide privacy from data collection by the providers for sharing with advertisers and other bodies.

Option 3: Generic Council Email Address (i.e. one address for the council):

The clerk can have an email account for the council which can be publicised on the website and in other places. Councillors do not use email for council business at all.

Pros: Easy to set up, promotes transparency, ensures continuity of communication.
Cons: Requires someone (often the clerk) to be responsible for monitoring the inbox, will not allow councillors to use email.

Select an Appropriate Format for Email Addresses

Community and Town Councils are elected bodies representing their communities in the same way as Unitary Authorities. A similar approach to that of Unitary Authorities should be adopted for emails for staff and councillors.

Some options could be e.g.

councillor**.**maryjones@community-cc.gov.wales

cllr.john.davies@comunity-cc.gov.wales

clerk@community-cc.gov.wales

david.williams@community-cc.gov.wales (where the clerk uses their name in their email)

Best Practices

Best operational practices for email use by councils need to focus on streamlined processes and clear procedures to enhance efficiency and effectiveness. Here are some key practices:

Email Management and Organization

Establish a standardized system for organizing emails. This includes creating folders and labels for different types of correspondence, setting up rules for automatic sorting, and regularly archiving old emails. An organized inbox reduces clutter and allows staff to quickly locate important information, thereby improving productivity.

Clear Communication Protocols

Define clear protocols for email communication, including guidelines on response times, the use of subject lines, and the appropriate use of 'To', 'Cc', and 'Bcc' fields. This ensures that emails are direct, relevant, and reach the intended recipients without unnecessary duplication. Many community and town councils have only a part time clerk or other staff. It is a good idea to create an automated answer to emails setting an expectation for timescales for a response e.g. if emails are only reviewed on a weekly basis.

Standardized Signatures and Templates

Implement the use of standardized email signatures and templates. This not only presents a professional image but also saves time and ensures consistency in communication. Templates can be used for common messages such as meeting summonses, issue of regular documentation such as agendas and minutes, and announcements.

Regular Training and Updates

Offer regular training sessions for staff on effective email management and communication strategies. Keeping up to date with the latest features of email platforms and best practices ensures that staff can utilize the tools available to them effectively.

Efficient Use of Email for Task Management

Consider the use of email in conjunction with task management tools. For example, using email to assign tasks and setting up follow-up reminders can help ensure that tasks are tracked and completed efficiently.

Technical and Security Considerations

Security Risks

Spam: Unsolicited emails that can clutter inboxes and reduce productivity. Spam often contains phishing attempts, which are fraudulent messages designed to steal sensitive information. Most email providers now offer spam filtering which will remove obvious spam messages. Staff and councillors should be conscious of spam and treat all email from unfamiliar senders with scepticism

Malware: Malicious software that can be delivered via email attachments or links. Malware can compromise systems, steal data, and disrupt operations. Most email providers now offer malware protection, but this is never complete. Staff and councillors should not click on links or download attachments from unfamiliar senders.

Data Loss: Emails can be intercepted or accessed by unauthorized parties, leading to potential data breaches. This risk is heightened if emails contain sensitive or confidential information. Encrypted emails can offer some protection but there are costs and complexities associated with its use. Community and Town Councils are not typically dealing with large amounts of sensitive information, and it is more appropriate that where such information needs to be sent then a method other than email could be used.

Phishing: A form of cyber-attack where attackers impersonate legitimate entities to trick recipients into divulging personal information, such as passwords or financial details. Staff and councillors should be conscious of this risk spam and be very careful before entering any personal or sensitive information which is requested in an email communication.

Ransomware: A type of malware that encrypts data and demands payment for its release. Ransomware attacks often start with a malicious email. Numerous large public and private sector organisations have been the victim of sophisticated ransomware attacks. Community and Town councils are probably not key targets for this kind of attack due to their smaller size and financial resources, but the risk should be considered. Regular “offline” backups of data should be taken e.g. to an external hard drive so that another copy is available in the event of a ransomware threat.

Technical Requirements

Hardware (Equipment): Laptops and desktop computers used by office staff employees need to be suitable to manage email applications. However, these are not applications that require a large amount of computing power so any reasonably recent device should satisfy this requirement.

Software and Services: A policy should be in place that all computing devices are equipped with up-to-date operating systems and that regular updates are applied to manage risks from malware and other online threats.

Version History

	Date	Issuer	Reason	Review Date
V1	21/11/24	Justin Horrell	Initial Version	21/11/25

Ariennir gan
Lywodraeth Cymru
Funded by
Welsh Government