Electronic Usage and Monitoring Policy

Contents

1. Purpose

1.1. This document aims to establish Carmarthenshire County Council's policy for the proper and effective use of electronic communication and collaboration tools, such as Email, Microsoft Teams and SharePoint. It details the monitoring processes, data retention practices, and approval protocols for access, information, monitoring, and investigations.

2. Scope

2.1. This policy applies to the usage of the Council's electronic communication and collaboration facilities, both for internal and external communication. It takes into consideration best practices, safety, and the cyber risks associated with data access, adhering to the principles of least privilege.

2.2. The policy applies to any devices, including Council-issued laptops, smartphones, iPads, and personal BYOD phones, which can access any of the Council's electronic communication tools for example Microsoft Outlook and Teams.

2.3. This policy governs the Council's approach to the management of these facilities, ensuring the best interests of both officers and elected members are upheld.

3. Policy statements

3.1. That Electronic Communication facilities will be used in accordance with:

3.1.1. This policy and related guidelines.

3.1.2. All appropriate Council policies - including the Information Security Policy, Handling Personal Information Policy, Breach Reporting and

Response Policy, Internet Usage and Monitoring Policy, and the Portable Device Usage Policy.

3.1.3. All appropriate legislation – including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, The Freedom of Information Act 2000 and the Computer Misuse Act 1990

3.2. All individuals, including employees, casual workers, agency staff, elected members, volunteers, external consultant or contractors, who use electronic communication facilities by the Council, must read and accept to adhere to this policy.

4. Responsibilities

4.1. All managers will be responsible for implementing the policy within their areas of responsibility.

4.2. All users of electronic communications are expected to pass on any relevant data from systems such as Emails or OneDrive prior to ending employment with the Council.

4.3. Digital Services will develop, maintain, and publish procedures and standards to achieve compliance with this policy.

5. Usage Principles

5.1. By using any of the Council's electronic communication and collaboration tools, such as Email, Teams, and SharePoint, you agree to this policy.

5.2. Secure methods of communication must be used if the content is of a sensitive, confidential or personal nature (e.g. it contains sensitive personal information). Further information and guidance can be found in the **Handling Personal Information Policy & Procedure.**

5.3. The Council provides these facilities to assist in the performance of their jobs and no personal use is permitted.

5.4. Correspondence made on Council-provided platforms will be treated as business correspondence and as such will be filtered, recorded and archived.

5.5. Council's internal emails and documents should not be forwarded outside the Authority unless it is necessary for conducting Council business. This also applies to sending copies of internal emails to personal email addresses.

5.6. Do not use Council's email addresses for personal accounts like Facebook or Amazon.

5.7. No employee, casual worker, agency staff, elected member, volunteer, external consultant or contractor, will send, forward or knowingly receive electronic communication that in any way may be interpreted as bullying, harassing, victimising, defamatory or discriminatory by any other person, or company, or which contravenes the Authority's **Behavioural Standards in the Workplace policy.**

5.8. Care must be taken when sending emails or sharing files. You must ensure that the correct recipient is selected and check that the email address is right. Please refer to guidance on Handling Personal Data that is available on the intranet.

5.9. Any breaches should be reported immediately to your line manager, **and** the Council's Data Protection Officer (databreaches@carmarthenshire.gov.uk) or the Chief Digital Officer.

5.10. Any messages sent from a logged-in account will be attributed to that user. You must log off or lock your computer when away from the desks.

5.11. If you have been given approval for a delegate to access your mailbox, you must provide precise instructions to delegates regarding their responsibilities and the proper use of the access. As the mailbox owner, you are accountable for the data contained within the mailbox, as well as any emails sent, information handled and/or received on your behalf.

5.12. Information obtained from a delegated or shared mailboxes must be kept confidential and should not be shared with others without explicit permission from the mailbox owner.

5.13. Shared/team mailboxes must have a mailbox manager/owner.

5.14. Shared Mailbox owner(s)/manager(s) are responsible for approving access requests to shared mailboxes, to ensure the requests are legitimate and that only those who require access are provided the relevant permissions based on business need.

5.15. Delegate permissions to mailboxes to be specified by the mailbox owner/manager based on business requirements and the principle of least privilege. (See Appendices 1).

5.16. All users must ensure compliance with all relevant legislation when using the Council's electronic communication and collaboration systems.

5.17. All documents and messages created and sent via Council's systems are owned by the Council and not by individuals.

5.18. Only open attachments from known sources and use caution with unexpected ones, even if they come from familiar contacts.

5.19. The facility to automatically forward emails must not be used to send messages to personal email accounts and external organisations

5.20. Electronic Communications will be managed by the Council to meet both its own requirements and any legal obligations for the storage and retention of data.

5.21. It is your responsibility to ensure the privacy of communications, such as emails, is maintained if you are working in an open area. This includes limiting who can view your device's screen when working remotely from any venue or from home, and that it is not visible or accessible to members of your family or the public.

6. Phishing Communications

6.1. Phishing communications are fraudulent messages designed to trick recipients into revealing sensitive information, such as passwords, credit card numbers, or personal details. These emails or messages often appear to come from legitimate sources

6.1.1. Email Verification

- Always verify the sender's email address. Be cautious of emails from unknown or suspicious sources.
- Check for inconsistencies in the sender's email address, such as misspellings or unusual domains.

6.1.2. Links and Attachments

- Do not click on links or download attachments from unknown or unexpected emails.
- Hover over links to see the actual URL before clicking.

6.1.3. Personal Information

- Never share personal or sensitive information (e.g., passwords, financial details) via email.
- Be wary of emails requesting urgent action or sensitive information.
- Be aware you could be contacted over Teams by someone unknown.

6.1.4. Reporting Phishing Attempts

- Report suspected phishing emails using the ‘report a message’ feature
- Contact the IT Service Desk if you are suspicious of any online activity.

6.1.5. Training and Awareness

6.2. You must complete the mandatory cyber security training that is available on the Council’s Learning & Development platform.

- Phishing awareness exercises will be undertaken to improve awareness of attacks.

6.2.1. Incident Response

- If you suspect you have fallen victim to a phishing attack, contact the IT Service Desk immediately.
- Follow the IT department's instructions to secure your account and prevent further damage.

7. Data Retention

7.1. It is your responsibility to adhere to good data hygiene principles. Emails that need to be retained as records should be filed on the appropriate SharePoint site. Obsolete emails should be deleted from mailboxes.

7.2. The Council's data retention policy explains how electronic communication data is managed and stored and details your compliance responsibilities. Data retention periods are listed on the intranet (See Appendices 3).

7.3. Documents and emails must be reviewed regularly, and any non-essential messages must be deleted in accordance with the Council's Retention periods (See Appendices 3).

7.4. Automated data retention policies are in place for Microsoft Teams. Messages will be deleted as follows

- Teams channel messages – 365 days
- Teams chat messages – 7 days

7.5. Quota limits are set on mailboxes. It is your responsibility to ensure you do not exceed this quote limit and that your mailbox is managed in an appropriate manner.

7.6. Manually deleted emails can be recovered from the "Deleted Items" folder within 30 days. After this period, they are permanently deleted and cannot be restored.

7.7. Documents stored on SharePoint Online and within Microsoft Teams can be recovered for a period of up to 93 days from the time of deletion. After this period, they are permanently deleted and cannot be restored.

8. Automated monitoring and filtering

8.1. The Council will automatically monitor email communication including both the text of a message and any attachments. The Council will monitor both incoming and outgoing mail.

8.2. Emails will undergo automatic content filtering, which may result in some emails being blocked from delivery. Users will receive notifications if an email is placed in quarantine.

9. Requests for Access, Information, Investigations and Monitoring of Electronic communications.

9.1. Requesting access to a staff member or elected members mailbox is not standard practice and should only be considered in accordance with this policy as a final option. Alternative methods, such as an 'Out of Office' notification or email redirection, should be explored first.

9.2. Requests will be documented by the Cyber Security Team to maintain an audit trail. The log will include details such as the reason for access, type of access, timeframes, due diligence, and consultation undertaken. An approval request will then be submitted to the Chief Executive through an electronic system. In the absence of the Chief Executive, the Assistant Chief Executive is authorised to grant approvals for staff, or the Monitoring Officer for elected members.

9.3. The **Chief Executive and Monitoring Officer** can authorise access to a mailbox under the circumstances outlined below. This is done in consultation with the relevant Head of Service and Director.

9.3.1. A request to add a delegate to access a mailbox.

9.4. When a staff member or elected official requests that an officer be granted access to their mailbox, they must clearly state the business justification, the required level of access (as detailed in Appendices 2), and the duration for which access is needed (e.g., one week, one month). The Line Manager and Head of Service and Director must be notified and provide their approval. For elected members, the Monitoring Officer must also be informed and give their consent. The request will then be submitted to the Chief Executive for final approval.

9.4.1. Staff absence.

To ensure business continuity and to obtain messages which require action during a period of absence, a line manager can request authorisation to access an absent employee's mailbox in exceptional circumstances. Both the Head of Service and Director must agree to this request. The employee must be informed by their line manager or if this is not possible due to the employee's condition, upon their return to work. The Chief Executive will be sent the request for final approval.

9.4.2. Investigations. Where an investigation is being undertaken, requests for access need to be formally approved as follows:

- Investigation into a Member of Staff: **Chief Executive**
- Investigation into an Elected Member: **Chief Executive and Monitoring Officer**

9.4.3. Monitoring. Where an electronic communication needs to be audited, monitored or tracked, requests need to be formally approved as follows:

- Tracking a Member of Staff: **Chief Executive**
- Tracking an Elected Member: **Chief Executive & Monitoring Officer**

10. Compliance measurement

10.1. Compliance with this policy is mandatory for officers and members. Breaches of this policy by staff may lead to disciplinary action being taken. Breaches by elected members may be reported to the Standards Committee.

11. Custodian

11.1. It is the responsibility of Digital Services to ensure that this policy is regularly reviewed and updated.

12. Version History

Version	Date	Actioned By	Revision Description	Approved By
Email Usage and Monitoring Policy v1	April 2016	John M Williams	Created new Policy	Executive Board on 20th June 2016
Email Usage and Monitoring Policy v2	May 2019	John M Williams	Updated policy to reflect changes	Exec Board Member - July 2019
Email Usage and Monitoring Policy v2	May 2022	Richard Williams	Reviewed Policy no changes	
Email Usage and Monitoring Policy v2	September 2024	Richard Williams	Reviewed Policy no changes	
Electronic Usage and Monitoring Policy v1	March 2025	John M Williams	Updated and renamed policy to Electronic Usage and Monitoring	Cabinet Member for Organisation & Workforce on 5th September 2025

13. Ensuring Equality of Treatment

13.1. This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, sex, gender reassignment, gender identity or expression, sexual orientation, parental or marital status.

If you require this publication in an alternative format, please contact Digital Services by emailing itsecurity@carmarthenshie.gov.uk

Appendices:

1. **The following provides the mailbox Access Rights/Permission Levels available for 'Shared/Team' mailboxes and an explanation of what each permission permits:**

   - **'*Read and Manage*'** permissions – allows a delegate to open your mailbox, read, move, and delete emails, create calendar events, and edit contact information in 'People' as if the mailbox owner. Emails cannot be replied to or sent with this permission.

   - **'Send on behalf of'** permissions – as 'Read and Manage' but also able to send and reply to emails on your behalf. The received email will state the email has been sent from your mailbox, on your behalf:

   - E.G. 'Sent by Emma Williams on behalf of IT Security.'

   - **'Send As'** permissions – as 'Read and Manage' but can also send and reply to emails. Message will appear to have been sent from the shared mailbox not the sender. **This is NOT granted to user mailboxes under any circumstances.**

     E.G. A member of the Cybersecurity Team sends an email by choosing the 'IT Security' mailbox within the 'From' box in Outlook. The received email will appear as to have been sent by the IT Security shared mailbox.

2. **The following provides the mailbox Access Rights/Permission Levels available for 'User' mailboxes and an explanation of what each permission permits:**

   - **'*Read and Manage*'** permissions – allows a delegate to open your mailbox, read, move, and delete emails, create calendar events, and edit contact information in 'People' as if the mailbox owner. Emails cannot be replied to or sent with this permission.

   - **'Send on behalf of'** permissions – as 'Read and Manage' but also able to send and reply to emails on your behalf. The received email will state the email has been sent from your mailbox, on your behalf:

     E.G. 'Sent by Emma Williams on behalf of IT Security.'

3. **Carmarthenshire Data Retention - Records Management**