Information Governance

Email Usage and Monitoring Policy

Contents

1. Purpose

1.1 The purpose of this document is to define Carmarthenshire County Council's policy for the effective and appropriate use of email.

2. Scope

2.1 Email usage refers to all use of the Council's electronic mail facilities whether for internal or external communication.

2.2 This policy governs the Council's approach to managing its email facilities, ensuring the best interests of both staff and the Council are upheld.

3. Policy statements

3.1 The Council's email facilities will be used in accordance with:

- This policy and related guidelines
- All appropriate legislation – including the Data Protection Act 1998, Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000.

3.2 Email usage will be monitored to ensure compliance with the email usage principles.

3.3 This policy is approved by, and has the full support of, the Council.

3.4 All permanent employees, elected members, volunteers, contractors and temporary staff provided with email facilities will electronically sign the policy to indicate their agreement to comply.

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

4. Responsibilities

4.1 The Council will provide staff with education and training to support compliance with this policy.

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

4.3 All employees and elected members provided with email access will signify their acceptance of this policy.

4.4 The IT Security Officer will develop, maintain, and publish procedures and standards to achieve compliance with this policy.

5. Email usage principles

5.1 The use of the Council's email facilities indicates acceptance of the policy.

5.2 It must be remembered that standard email is not a secure form of communication. The messages that you send may be sent over networks owned by other people and can be intercepted, and read by someone else. A secure method of communication must be used if the content of an email is sensitive (e.g. it contains sensitive personal information), such that if its content were disclosed to or modified by an unauthorised person, it could cause harm or distress. Further information and guidance can be found in the **Handling Personal Information Policy & Procedure.**

5.3 The Council provides email to assist employees and elected members in the performance of their jobs and no personal use of email is permitted. Staff should make use of internet based email for their personal requirements and usage of these sites should be in line with the **Internet Usage and Monitoring Policy.**

5.4 All emails will be treated as business correspondence and as such will be filtered, recorded and archived.

5.5 Users must not register any Carmarthenshire County Council email address with any site or system that is not work related, such as a personal Facebook / Ebay account.

5.6 The Council reserves the right to purge identifiable personal email to preserve the integrity of the email systems.

5.7 No employee, elected member, consultant or contractor will send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company, or which contravene the Authority's **Behavioural Standards in the Workplace policy**.

5.8 Care must be taken when sending emails. Users must ensure that the correct recipient is selected (if selected from the address book) and ensure that the address is correct before sending.

5.9 The user logged in at a computer will be considered to be the author of any messages sent from that computer. Users must log off or lock their computers when away from their desks.

5.10 Under no circumstances must emails be sent from an account that the user does not have the authority to send from as this is an offence under the Computer Misuse Act 1990.

5.11 All email traffic, including attachments, will be automatically monitored and reviewed, and any disciplinary action deemed appropriate will be taken.

5.12 All users must ensure compliance with all relevant legislation when using the Council's email system.

5.13 All documents and messages created and sent via the Council's email system are owned by the Council and not by individuals.

5.14 Email folders must be reviewed regularly and any non-essential messages must be deleted in accordance with the Council's **Retention Guidelines**.

5.15 Internal email and other internal materials must not be forwarded to destinations outside the Authority unless this is done in the course of performing the business of the Carmarthenshire County Council.

5.16 Users must not forward chain letters either internally or externally. This includes those purporting to be for Charity or other good causes as well as those promising wealth or other personal gain. Virus warnings come under the same exclusion as the majority of these are false. Employees must refer to the IT Security Officer to check the validity of such messages but must not forward these messages to anyone else inside or outside the Authority under any circumstances.

5.17 Email addresses must not be disclosed unnecessarily. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.

5.18 Users must not subscribe to email lists unless they are work related. The volumes of messages that can be generated are high and the content may be dubious resulting in conflict with the conditions stated above.

5.19 Email must not be used to send large attached files. Many of the staff are working in offices at the end of slow communication lines and large emails will slow down these links even further. Many email systems will not accept large files and, if returned, may result in overloading the Council's own email system. Users should store files on shared network drives/Corporate File Plan and send links to the documents in their emails for internal recipients.

5.21 Emails and attachments should not be opened unless they are from a known source. Caution must also be exercised even if attachments are received from a known source but are unexpected.

5.22 The facility to automatically forward emails must not be used to forward messages to personal email accounts. The Council provides a number of solutions for accessing its email system when away from the office. Advice must be sought from IT if remote access is required.

5.23 Emails will be managed by IT to meet both its own requirements and any legal obligations for the storage and retention of messages.

6. Email monitoring

6.1 The Council's email facilities will be monitored in accordance with:

- This policy and related guidelines
- All appropriate legislation – including the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7. Automated monitoring and filtering

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

7.2 Emails will be automatically filtered according to the content and as a result may even be blocked from delivery. Users will be automatically notified if a message has been blocked.

7.3 Regular summary reports on email usage will be made available to managers. More detailed reports will be made available on request by Heads of Service

8. Requests for information, investigations and tracking

8.1 The Head of Service, Director or Chief Executive can authorise access to a

member of staffs mailbox based on the circumstances outlined below.

8.2 Staff absence. Where a member of staff is absent from work, authorisation can be given for the staff members line manager to have access to their email. Normally such access should only be sought for absences in excess of 10 working days. The "owner" of the Mailbox should be informed immediately by their Manager of the access being allowed.

8.3 Investigations. Where an investigation is being undertaken which could result in **Gross Misconduct**, requests need to be formally signed off as follows:

- *Member of Staff: Director Approval*
- *Elected Member: Monitoring Officer (who will inform the standard committee)*

8.4 Tracking. Where an email needs to be tracked to identify where it has been sent, requests need to be formally signed off as follows:

- *Member of Staff: Director Approval*
- *Elected Member: Monitoring Officer (who will inform the standard committee)*

9. Compliance measurement

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

10. Sponsor

10.1 This policy is owned by the Corporate Information Governance Group.

10. Custodian

10.1 It is the responsibility of the IT Security Officer to ensure that this policy is regularly reviewed and updated.

11. Ensuring equality of treatment

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

If you require this document in an alternative format please contact the IT Security Officer on 01267 246311 or email **ITSecurity@Carmarthenshire.gov.uk**

Policy approved by Executive Board Member on: 14th May, 2013
Policy review date: November, 2015
Policy written by: Idris Evans CISSP
Reviewed by: John M Williams CISMP