Email Management Policy

Document Control

File Name	Email Management Policy
Original Author(s)	Nia N Thomas
Current Revision Author(s)	

Version	Date	Author(s)	Notes on Revisions
V1.0	10/02/2010	Nia N Thomas	
V2.0	19/02/2010	Noelwyn Daniel	
V3.00	16/03/2011	Noelwyn Daniel	
V4.0	03/06/2016	Nia N Thomas	

Introduction

Increasingly, wherever email can be readily accessed, the business of Carmarthenshire County Council is being transacted by individuals using email. Consequently, email correspondence is now being routinely used to transact and record decisions that were previously often in paper form only; emails are frequently the only record of these transactions. In this context email and their attachments are records of value and need to be managed within the authority's records management system like any other record. The medium is irrelevant. The content of the message determines whether it is a record or not; the content determines to which records series the message belongs; and the content determines how long the message needs to be retained.

Purpose

The document sets out the policy of Carmarthenshire County Council (the Authority) in relation to email management. The policy applies to all users, and others given permission to use the Authority's email, and is designed to supplement the policies on Internet and email use.

This policy should be read in conjunction with the Email Management Guidelines and the Records Management Policy, which state how the Authority will manage its records, including electronic records.

Personal Folders

The creation of Personal Folders (*.pst files) will not be permitted. The creation of Personal Folders (*.pst files) not only allows emails that are not records and those that are past their retention date to remain, but they allow emails to be contained within an unmanaged and inaccessible local silo.

Mailbox size
Outlook mailboxes will be increased to 500Mb for all staff and 1Gb for Heads of Service.

Retention
Email records should be saved from Outlook into the appropriate file plan according to their content and managed in a consistent manner to all other corresponding records. If the email is not relevant for business purposes it should be deleted. An email is important if it:

- Has long term administrative or historical value.
- Contains information, advice or explanation not duplicated elsewhere.
- Relates to decisions taken and has evidential value.
- Was drafted as a result of policy or legislation.

All email records are subject to the Authority's retention schedules according to their content and should be destroyed, or transferred to the County Archive Service for future preservation, once they are no longer of operational use. The retention schedules can be found on the intranet.

Authenticity
Email records should completely document the transaction. Complete email records must include all of the following elements, as applicable:

- Recipient(s)
- Sender
- Subject
- Text
- Date sent
- Time sent

The contents of the email record should accurately reflect the transaction.

Accessibility
All email records, like other electronic records, should be reasonably accessible for the purposes of FOIA, Data Protection, Subject Access requests and legal disclosure.

The email record should be easy for users to manage as part of the daily workflow and records management practices.

Disclosure
Email is part of the corporate record of the Authority and as such is liable for disclosure in response to information access requests under the following legislation:

- Data Protection Act 1998
- Freedom of Information Act 2000.
- Environmental Information Regulations 2004 - information regarding this legislation can be found at http://www.informationcommissioner.gov.uk/

Disposal
The process of deleting emails must be comprehensive, complete and irrevocable. The guidance from the Information Commissioner's Office is explicit in its assertion that:

> *"Information located in desktop recycle bins is clearly subject to the FOIA as this continues to be held and is easily accessible. Once deleted from the recycle bin the information will also continue to be held unless the electronic record is completely erased from the computer system."*
>
> *"Information in a deleted file or in a back-up, whether a server, disc or tape, may be regarded as being held by a public authority for the purposes of the FOIA depending on the particular circumstances of the individual case.*

Attachments
Wherever possible attaching documents to emails must be avoided, users should insert links to documents from the file plan.

Training
All new employees will be trained on email management as part of their approved induction programme. Users will be trained to:

- create fewer emails
- identify email records
- save email records to the corporate file plan
- send links instead of attachments

Guidance will be published on the intranet.

Security
The email record should reside in a secure system that controls access, storage, retrieval, alteration, and deletion. Email records present unique security concerns, because email messages are:

- Easily manipulated or deleted in the system
- Easily captured and read by unintended persons

- Easily forwarded and misdirected by mistake

This policy also applies when using non-County Council resources.

Monitoring
The Authority will endeavour to follow the policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be a regular planned audit to assess how the policy is being put into practice including monitoring the use of attachments in emails.

Evidence

Users should be aware that email messages could potentially be used as evidence in legal proceedings. In addition the Authority could also be liable for any negligent advice given by email, just as through other means of communication.

Users should note that they may be personally liable to prosecution and open to claims for damage should their actions be found to be in breach of the law

Responsibility
It is the responsibility of all users to ensure that corporate policies and procedures for managing records including emails are adhered to. All users should familiarise themselves with the content of this document to ensure that their interests and those of the Authority are protected. It is the responsibility of each individual to ensure that the guidance set out in this policy and Records Management policies is adhered to at all times.

.

.