The National Archives

Guidance principles on the auto-deletion of email

This publication is available for download at nationalarchives.gov.uk.

This document sets out the guiding principles for the auto-deletion of email. It sets out what emails can be deleted and what technologies can be put in place to assist departments. It forms part of The National Archives' existing suite of guidance on managing emails.

To delete or not to delete?

- Emails of historical value and enduring public interest should be kept
- However, email volumes can become unmanageable, leading to real problems. For example:
    - there is a risk of a breach of the Data Protection Act if emails contain personal or sensitive information
    - information retained long term in mailboxes may pose more of a security risk
    - they can be difficult to search and find information in
    - storage capacity can become limited and costly
- Auto-deletion can be a useful tool in managing email volumes. It can reduce the need for manual processes which can often fail due to lack of time, resource and priority
- An auto-deletion policy can also encourage users to actively consider which emails have ongoing value and therefore need to be captured in the department's EDRM solution

What are the options?

Once you have identified why you need to delete emails the next thing to consider is how to apply this practically. This will differ for each department, currently ranging from 90 days to four years.

Departments should bear in mind that it may not be possible to use a blanket auto-deletion process due to ongoing litigation or inquiry.

The auto-deletion options are:

1. **Deal with the ephemeral items first –** Set up policies for deleted, sent and calendar items with shorter time periods or allow staff to manage these time periods themselves. This gives the users some flexibility to manage their own inbox – they know that items will be deleted by default after two years but can assign shorter periods to certain folders that they know will not be required as long.

2. **Set up a non-deletion area or archive –** Consider creating a separate folder or area that is not subject to the auto-deletion policy; this will need to be well governed and monitored to ensure it is not abused or used as a dumping ground. Emails subject to further investigation or legal hold can be placed in this area to ensure the information is not lost. Ensure the area is searchable so there are no problems with e-discovery or requests for information.

3. **Set up rules and expiry dates on unwanted items –** Advise users who regularly send out emails with general office information and announcements (events happening, building changes, fire bell tests, IT changes, etc.) to consider applying expiry dates to the emails they send. Your IT department can arrange for these to be automatically deleted once that date/time has been reached.

4. **Email is not the only option –** Where appropriate make use of instant messaging, collaboration areas and intranets to exchange and share information. Although these present their own challenges for the management of information they may be suitable for short term correspondence, announcements or knowledge sharing where retention of a permanent record is not required.

5. **Automatically capture emails –** Implement technologies that integrate your email and EDRM solutions. Solutions that allow emails to be dragged and dropped or automatically captured into the corporate records area will assist in allowing users to comply with your records management and retention policies.

What are the risks around an automatic deletion policy?

Information Loss:

Information of a business and/or historic value could potentially be lost as a part of an auto-deletion policy. It is important that staff are clear what emails should be kept. However, information may be lost anyway if there is no auto-deletion policy in place, for instance, if inboxes are deleted if a member of staff leaves. Under an auto-deletion rule information of value must be identified and not deleted.

Legislation and Regulatory Compliance:

Information that needs to be maintained should be transferred into your EDRM or network drives to ensure you are compliant with your retention policies. If you are implementing a blanket 90 day delete on mailbox items you need to provide assurance that none of the deleted information should be kept. In addition, your department may have separate regulations on the retention of email for auditing purposes.

Reputational risk can also play a part, particularly if dealing with Freedom of Information (FOI) requests, and information is perceived to have been deleted in response to a request for information.

Information is not deleted:

There is a risk, particularly when using third party agencies and cloud providers, that the information is not deleted but moved/archived to a separate area. If so, emails could still be subject to discovery and need to be managed appropriately. Ensure that your service-level agreement with the third party provider covers the requirement for the deletion of information and that they can prove that this has taken place.

People find a way around it:

If the policy is not effectively communicated and managed then users may become frustrated and find workarounds. Giving users plenty of notice that the policy is coming in and adopting a phased approach may assist with this. A good change management and training plan will help in getting users to 'buy-in' to the policy and avoid them seeking other ways around it.

Auto-deletion process at a glance

- Agree a deletion policy that works for your department and regulatory requirements
- Consider the risks of implementation against doing nothing
- Communicate and get support from the users
- Agree an implementation plan
- Agree a policy that works with your Records Management and Retention guidelines