Email Retention Policies Explained for UK SMEs

Why email retention matters

- For several reasons, email is integral to a UK business, including its Use for Contracts, Orders, Staff Communication & Financial Instruction.
- Many SMEs store Every Email they have ever received, sure that they may need or want to refer to them later.
- However, when you have many emails stored, it increases the Cost of Storing all those Emails as well as the Risk from Security Breaches.
- It can also cost a lot of time to find the email or information you are looking for when your mailbox is Large in Size.
- An Example of this: If your Mailbox is Hacked and you have thousands of Emails Stored, it would make the total damage from the Hack even more Severe.
- Additionally, Thousands of Emails make it more Difficult for a Business to Manage a Subject Access Request (SAR).
- Businesses are expected to Retain Personal Data only for the Length of Time Necessary as required by UK GDPR.
- The Information Commissioner's Office Expects A Business to have A Well Defined and Documented Email Retention Policy.
- Retention means that a Business will Maintain Emails for Important Business or Legal Reasons and Remove Unwanted Emails from its Email System.
- An Appropriate Email Retention Policy will help A Business be More Organised, Reduce Their Risk, and Comply with Data Protection Legislation.

What an Email Retention Policy Is

An email retention policy outlines the rules for:

- How long to retain various types of emails.
- The procedure for deleting emails.
- Special exceptions (i.e., legal holds).
- Who will follow the rules.

The purpose of an email retention policy is not to delete emails -- it is to be intentional about retaining the appropriate type of emails for a specified amount of time. Examples of email retention periods are:

- 6 years for customer sales emails for tax and/or insurance purposes.
- 12 months for internal administration emails.
- 6 years from the date of termination for HR Discipline emails.

The email retention policy will help you comply with the storage limitation principle of the UK GDPR and also assist with responses to Subject Access Requests or audits.

Why Keeping Emails Forever Is a Problem

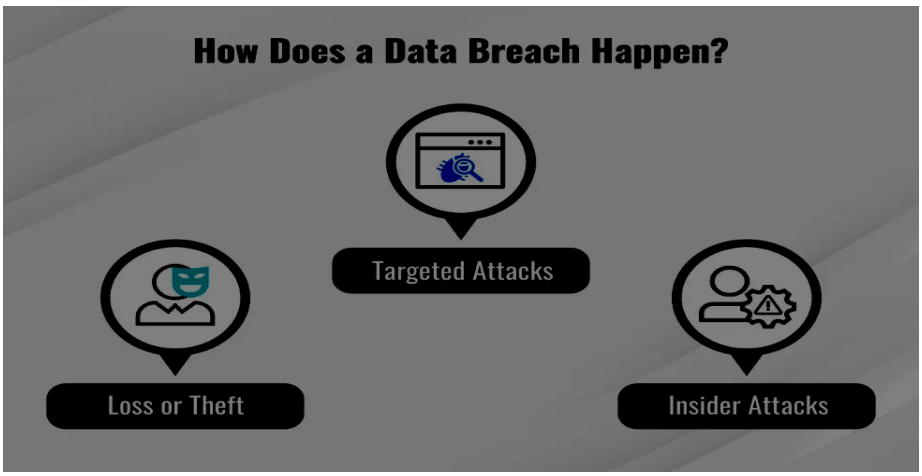
It is very tempting to keep emails just to be on the safe side, but holding an email permanently can create many problems, including:

- **Email Storage Cost:** This is growing quickly as the cost to store additional email in the cloud increases rapidly once the basic storage limit (base) is exceeded by use of cloud based solutions such as Microsoft 365.
- **Email Security Risk:** Data that is retained will be used in the event of a breach, and old emails may also contain sensitive personal information (e.g., credit card numbers, national insurance numbers, medical information).
- **Compliance Burden:** When there are requests from individuals for copies of their data, the more data held will result in having to provide all records that have been retained.
- **Email Productivity Drag:** Large mailboxes make it difficult to search email, create clutter and generally make it harder to effectively use Outlook or Gmail so this will slow down the use of email.
- **Increased eDiscovery Costs:** In the event of a dispute or during investigations, any archived emails that have not been culled raises our eDiscovery costs.
- **Legal Compliance Risk (GDPR):** The ICO considers any email retained indefinitely as a breach of the storage limitation under GDPR and thus while the usefulness of this information to the organisation decreases over time would normally be subject to warnings and it's unlikely that the ICO would impose a fine, if the company is a small entity it is possible that the ICO will impose a fine.

Risks of Poor Email Retention Management

Threats arising from ineffective management of email retention:

1. **Data breaches:** Having old emails potentially places unnecessary data in high danger.
2. **ICO enforcement:** If you can't provide a valid reason to keep data or fail to delete it once it isn't needed any more, ICO has the authority to issue penalty notices or levy fines against your business (for small businesses, the typical fine is £1,000 - £10,000).
3. **Delays in SAR:** Search for several years of emails requires a significant amount of time to perform, and must be provided within 30 days.
4. **Legal action:** Courts/insurance companies expect you to retain information for a reasonable amount of time retaining too much could make your position less defensible.
5. **Inefficient work processes:** Your staff spends valuable time searching through messy email inboxes.



How Email Retention Supports Compliance and Security

A retention policy that is both efficient and effective helps your business stay compliant with the following:

- **Limitation on retention of data as per UK GDPR Directive:** Only keep data for as long as necessary
- **Minimising Data:** Deleting what is not needed = Less Data to Keep Safe.
- **Security:** The smaller your archive the less impact of any security breach.
- **Support of Cyber Essentials:** Secure data configuration (keeping less old data means less chance of your system being subject to the vulnerabilities found in older software).
- **Insurance:** Many cyber insurance providers demand documentation to confirm evidence of suitable data management practices.

Typical Email Retention Periods for Different Business Functions

These times are general examples be sure to always use your legal obligations, needs of the business and risk assessment as a basis for how long emails are retained:

- **Finance and accounting email communication (invoices, receipts, tax records):** 6-7 years (required by HMRC for most records).
- **HR and employment records (contracts, discipline, payroll):** 6 years from end of employment (limitation period for claims).
- **Customer service and support email communication:** 2-6 years (depends on contract length and warranty periods).
- **Email negotiations and signed contracts:** 6-7 years after contract has ended.
- **Internal operational email communication (general admin, not-critical):** 1-2 years.
- **Marketing email communication (sales emails, promotional emails):** 1-3 years or until consent is revoked.

Document the reason why you intend to keep the email e.g. "Finance emails to be retained for 7 years to meet compliance with HMRC".

Most SMEs can set basic policies in under an hour.

How Email Retention Works in Modern Cloud Systems

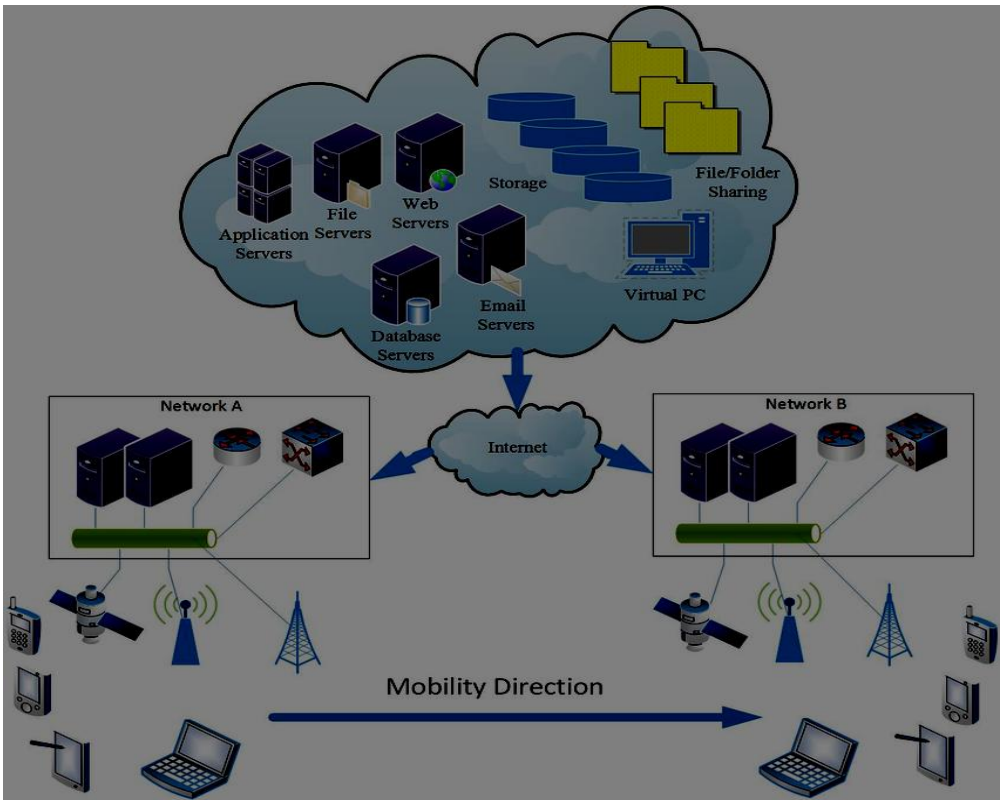
The top two solutions available for Small and Medium Enterprises (SMEs) in the UK, Google Workspace and Microsoft 365 both have built-in capabilities to help with Retention of email:

- **Retention policies:** Automatically retain and delete items, based on the length of time stored
- **Retention labels:** Can be applied to specific items (or items in folders) such as "Finance - Keep for 7 years".
- **Litigation Hold:** Prevents the deletion of items on hold while any lawsuits against your company are being resolved
- **Recycle bin & Versioning:** Allows for recovering deleted items for a period of time (OneDrive for example will keep for 93 days).

It only takes a few steps to apply Retention:

1. Open Microsoft 365 Compliance Centre → Data Lifecycle Management → Retention Policies
2. Click on the button to Create a new Policy → choose which location(s) the policy applies to
3. Establish a Retention Period and Retention Action (Keep or Delete).

For the average SME, setting up basic Retention Policies can be completed in less than an hour!



Simple Email Retention Policy Template

1. Policy Purpose

To ensure that the emails we keep contain information we need for business purposes, as determined by legal, regulatory and compliance constraints relating to how long we can store personal data in accordance with the UK GDPR principle of "Limitation of storage".

2. Scope

This policy applies to all staff, contractors and any other person who has been given access to Company email accounts.

3. Retention Principles

- Emails must be retained only for legitimate business purposes
- When emails are no longer needed they must either be deleted or archived
- Retention will be determined by the content and purpose of the email, not the identity of the sender
- Each retention period must have appropriate documentation to justify the retention period.

4. Retention Periods by Category

- Financial and Accounting: 7 years
- Human Resources and Employment: 6 Years after Employment Termination
- Contracts with Customers and/or negotiations with customers: 7 years after Termination of Contract
- Customer Support Related Emails: 3 Years
- Marketing Emails / Communications: 2 Years from the date sent, or until the customer withdraws their permission to receive emails.
- General (Admin - Non-Critical) Emails: 1 Year
- Legal / Regulatory: Retention of Emails is based on specific legislation.

5. Archiving and Storage

- If an email is still needed after [some years], it will be archived on an automatic basis.
- Use Microsoft 365 retention policies to enforce compliance.
- Only employees who are given access to archived emails will have access to them.

6. Deletion and Disposal of Records

- All records will be automatically deleted once their retention period has expired, unless there is a legal hold placed on them.

- The platform responsible for the records will handle their secure deletion.
- Records cannot be deleted manually without prior approval.

7. Legal Hold Procedures

- When litigation or a potential investigation is likely to occur, a legal hold can be placed on the records by a Director until such time as they are lifted.
- The implementation of the legal hold will prevent any further deletion of the records until such time as the legal hold is lifted.
- IT and compliance teams must be notified of the implementation of the legal hold as soon as possible.

8. Staff Responsibilities

- Staff will adhere to this policy when using records on a daily basis.
- Staff will flag any emails that they feel should be retained for a longer period of time than stated within the policy.
- Any employee who suspects that there has been a breach of this policy must report the breach immediately.

9. Monitoring and Review

- This policy will be reviewed annually, or at least every three years, or whenever there is any major change in legislation or the organisation's business model.
- Compliance checks will be conducted every quarter to ensure adherence to the policy by employees.
- Employees will receive annual training on this policy. (see above)

Signed Acknowledgement

I have read and agree to abide by the terms of this policy.

Name: _____ Date: _____

Common Mistakes Businesses Make

- Storing everything indefinitely → expenses and increased risk of storage failure.
- Over deleting → relevant evidence and related documents may be lost.
- No policy in place → practice is inconsistent and will be difficult to defend to the ICO.
- Ignoring legal holds → documents may be deleted by accident during any dispute.
- Assume a cloud-based solution handles everything for compliance/retention purposes → you need to ensure the cloud solution is configured correctly.

Email Governance Checklist for Directors

Directors should ensure:

- Documented email retention policies are in place at their organisation
- Their organisation has adequate email retention controls in place
- Staff know to protect sensitive information as outlined in their policies
- Staff have been trained regarding the policies related to email retention
- Policies are reviewed on a regular basis

FAQs

1. Is it obligatory to retain emails for businesses?

Although it isn't a specified time frame, you' have to hold onto data as long as is needed for its purpose (storage limitation under UK GDPR). Lots of companies hang on to Finance/HR data for 6-7 years due to taxation/limitation.

2. How long are emails held by companies for?

This depends on the content and purpose and so finance may typically be retained 6-7 yrs , HR usually keeps them for 6 yrs after employment, and customer support methods may be retained for 2-3 years. Make sure that your retention reasons are identified in accordance with the level of time to be retained.

3. Do employees have permission to delete business emails?

Only if this is specific within your policy, business email belongs to the business, thus by auto retaining emails, you prevent any accidental deletion from occurring.

4. Are email archiving and retention identical?

Archiving emails is simply transferring older emails to a cheaper method of storing data, while retention recording your holding timeframe of emails whether archived or deleted.

5. Will my cloud solution manage retention automatically?

No - Microsoft 365/Google have tools available but will require their policies/labels to be configured. Their default settings do not delete items.

6. What if I need to have access to my emails for legal reasons?

You will need to apply a hold, this will prevent anything from being deleted until the issue is resolved. You need to document the hold.

7. How will I make sure I receive Subject Access Requests?

You will need to conduct an all-source search of your information including any archived data and provide it within 1 month. Retaining the data will make it easier to respond to requests.

8. Is it appropriate to keep my emails forever for "just in case"?

This is not a best practice under GDPR and should only be retained for valid purposes.

About This Guide

The **Computer Support Centre** has created this guide for small and medium-sized businesses (SMEs) in the UK, to help provide a clear, easy-to-understand guide on how to create email retention policies. This document outlines how to manage email storage in an acceptable manner, how to support the principles of data protection and how to minimise risk by storing large quantities of historical email data.

This is a guide for business owners, managers, HR teams and IT providers to help them implement a sensible approach to email retention, with a focus on simplicity and avoiding unnecessary complexity.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

Email is an essential part of business communications, but retaining emails indefinitely can lead to numerous compliance, security and operational issues. Having an email retention policy that is clear and that provides guidance on how long to retain emails will enable businesses to retain emails for the appropriate amount of time while ensuring that all unnecessary email data is securely disposed of.

Establishing defined retention periods, utilising the tools available in modern day email platforms and ensuring all staff are informed of their responsibilities, UK SMEs will be able to improve the governance of their data, reduce their risk and manage business communications more effectively.