Email Migration Checklist for UK Businesses

Executive Summary

- Migrations involve switching to a new email service provider for your business.
- Most problems with email migration occur because of insufficient planning. Technology failures are rarely the reason for the disruption, missing data, or a delay in getting the new email system up and running.
- You should always back up your email prior to migrating, especially if you're using a cloud provider.
- Domain Name System (DNS) changes determine where your email will be delivered, and errors made while making these changes can cause all of your email to be stopped.
- You need to have an increased level of security in place during the migration (MFA, password management, admin controls).
- User communications are as important as the technical configuration for the email system.
- When you process customer data under GDPR, you must continue to protect that data as required even during and following the changes made as a result of moving to your new Cloud Email Service Provider.
- If you have a simple, structured plan to follow over 30 days you will limit the impact on your business from the email service provider migration.

Who This Guide Is For

This guide has been prepared for the following audiences:

- UK small and medium size businesses (1 – 50 employees)
- Owner-managed businesses
- Office Managers responsible for IT
- Financial Managers responsible for Technology
- Non-technical decision makers

No technical experience is required to follow the criteria contained in this guide.

What You Will Achieve

After reading this guide, you will:

- An understanding of what "email migration" means in layman's terms
- Knowledge on how best to prepare for the email migration process
- How to avoid the most common pitfalls during an email migration.
- How to keep your data safe and preserve the continuity of your operations during the email migration process.
- Improve your email safety during the email migration process.

- Understand the GDPR aspects to consider when undertaking an email migration.
- A plan for completing your email migration (30 Day Plan).

What Is Email Migration?

Email migration is defined as the movement of data:

- Mailboxes
- Contacts
- Calendars
- Shared mailboxes
- Distribution Lists

From one email platform to another.

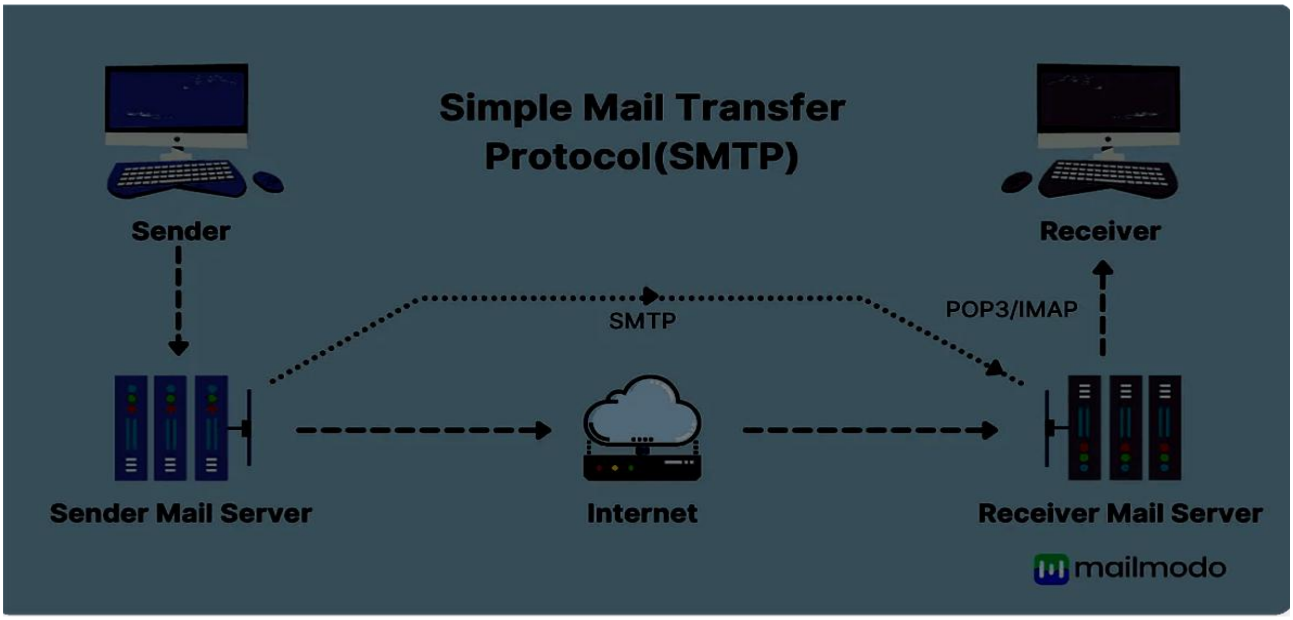
Common examples in the UK for Small to Medium Enterprises:

- Moving from an old hosted Exchange provider to Microsoft 365
- Migrating from on-premises Exchange to Cloud Email
- Migrating from one provider to another due to cost or service issues.
- Consolidating (combining) multiple domains into one.

When email migration is completed properly, the result for users will be minimal interruption.

When completed incorrectly the result will be:

- Missing folders and or lost emails.
- Downtime
- DNS (Domain Name System) Issues (mis-routing)
- Security Exposure



- GDPR (General Data Protection Regulation) non-compliance) Reporting Issues.

Planning & Preparation

The majority of migration-related issues can be averted with proper planning.

Establish the scope and goals.

- Make a list of any email accounts you now have, including email aliases, shared mailboxes and distribution groups.
- Determine your new email platform. (For many small and mid-sized businesses in England, Microsoft 365 Business Premium is the email platform of choice.)
- Establish your success criteria. (For instance: no email accounts lost; minimum downtime of less than four hours; all users trained in the use of the new system.)

Choose the migration methodology.

- Cutover (simple and accomplished in one step good for companies with fewer than 50 employees).
- Staged/hybrid (less complex but subject to יותר risk gradual)
- IMAP – recommended for migrating mail from source systems other than Exchange; third-party tool.

Begin the backup process.

- Export All items to PST or create a back-up of your mailboxes using either an Outlook or admin tool.
- The current settings must be backed-up or you will need to take a Picture of them (MX Records, SPF, DKIM, DMARC) so they can be restored when you migrate.
- The current provider is the partner. Therefore, they can provide both a backup copy of your mail server. Backup is available for most current providers.

Notify all Stakeholders.

- Advise all employees of dates and details about what to expect.
- If there are changes to shared email addresses, inform any key clients or suppliers affected by those changes.

Prepare the DNS and domain.

- Verify that you are in control of the DNS (registrar or hosting company).
- Validate the MX records are pointing to the old email service provider.

Migration Steps

1. Tenant Setup

What it is

How to set up a new email account (Microsoft 365) environment.

What do you need to do to get your tenant set up?

- Verify the domain
- Create users
- Assign licenses
- Create basic security settings

Why it matters

If configured incorrectly:

- Email cannot be delivered
- Security holes will exist
- Users cannot get into their account

Common mistakes

- No account naming standard for manually created accounts
- No MFA from day one
- Shared mailboxes are not set up

Quick wins

- Create a MFA for all users immediately
- Create a naming standard for all users (i.e., first.last)
- Create your admin account separate from a user account

2. Mailbox Migration

What it is

Moving email, calendar and contacts to your new environment.

Migration type varies on the provider:

- Cutover migration
- Staged migration
- IMAP migration
- 3rd party migration tools

Why it matters

there is any incomplete data:

- Missing folders
- Corrupt data
- Lost historical email

Common mistakes

- Mailbox size limitations are not checked
- Migrate with no test account first
- Don’t forget to migrate archive mailboxes

Quick wins

- Migrate 2-3 test accounts as pilots before migrating all mailboxes
- Confirm that all folders transferred
- Confirm sent items are on all accounts

3. DNS Changes

What it is

Completely reconfiguring your domain's MX Record to ensure email can be sent through to the new system.

Why it matters

If done incorrectly:

- Emails will stop being sent
- Email messages will bounce back to the sender
- Customers will not be able to reach you

Common mistakes

- Incorrectly identifying the MX priority
- Not updating the SPF record
- Forgetting to add an autodiscovery record
- Not updating your DKIM / DMARC records

Quick wins

- Double check the MX value before saving
- Add the new provider’s SPF record
- Test for External Email Once the Change Has Been Made

DNS propagation may take 24 hours (often faster so test immediately).

4. Security Configuration

What it is

This is your opportunity to upgrade the overall security of your environment.

Minimum Standards

- MFA Enabled
- Strong Password Policy
- Legacy Authentication Disabled
- Restrict Administrative Roles

Common mistakes

- Delaying MFA implementation
- Leaving Global Admin Rights assigned to too many users
- Ignoring the use of Conditional Access Rules

Quick wins

- Implement MFA Before MX Record Cutover
- Remove Global Admin Rights From Standard Users
- Disable Basic Authentication

5. User Communication & Training

What it is

Prepping staff for change.

This part contains:

- Login instructions
- MFA setup help
- Instructions for new app
- Mobile phone instructions

Why it matters

Users being confused are:

- Help desk overload
- User lockout
- Frustration
- Decrease in productivity

Common mistakes

- Not providing training
- Not creating written documentation
- No having support contact information

Quick wins

- Send one-sentence e-mail to users “What to Expect”
- One-page login guide
- 30-minute Q&A

GDPR & ICO Considerations

Email contains personally identifiable information.

During migration:

- Data is in process
- Data may move outside the UK
- Data may temporarily be stored in third party tools.

Under UK GDPR:

- You still own the data.
- You will make sure all people processing the data are complying.
- You should have appropriate protections for international transfers.

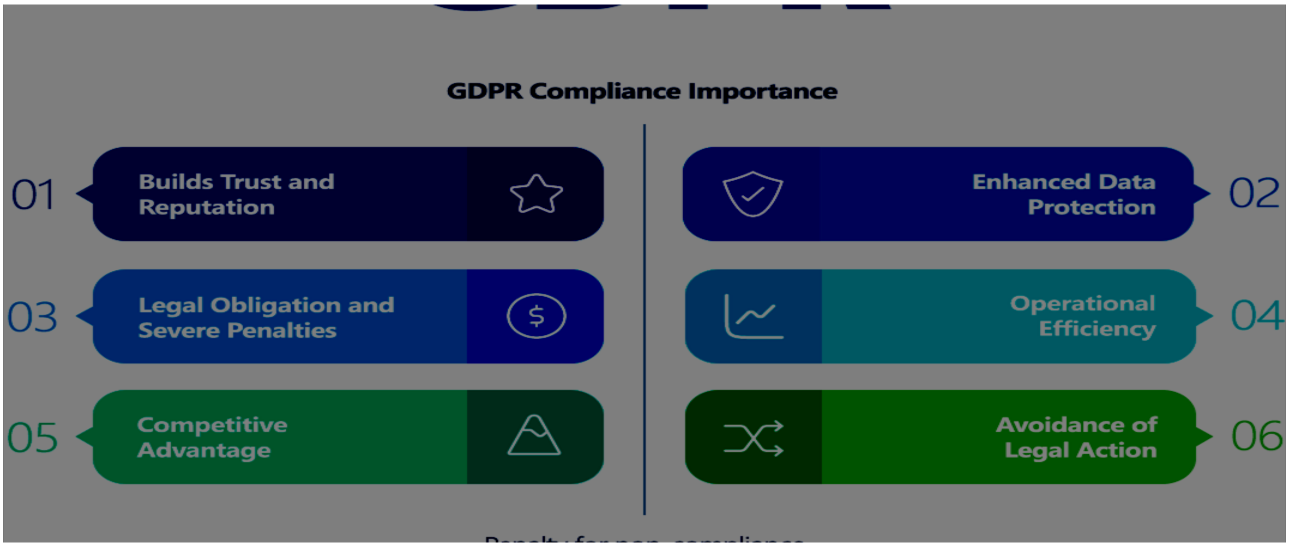
If data is lost during migration, and includes personally identifiable information:

- You’re required to notify ICO within 72 hours.
- You should notify affected users.

Before migration:

- Confirm new provider’s UK GDPR compliance.
- Confirm where data will be stored.
- Review Data Processing Agreement (DPA).

- Confirm data will be encrypted in transit.


GDPR Compliance Importance
01
Builds Trust and Reputation
02
Enhanced Data Protection
03
Legal Obligation and Severe Penalties
04
Operational Efficiency
05
Competitive Advantage
06
Avoidance of Legal Action

Post-Migration Checks

Be sure to check that everything is running properly after cut-over.

An example of a checklist may include:

- Test sending TEST Email both internally & externally
- Verify immediate sync of all mobile devices.
- Verify accessible Shared Mailboxes
- Verify Correct Calendar Sharing
- Verify proper SPAM filtering.
- Review of Audit Logs.
- Confirm proper operation of Back-Up System
- Revoke access from previous provider

Troubleshooting Common Issues

1. **Problem:** All e-mails are bouncing off?

Cause: Wrong MX/SPF settings.

Fix: Re-check the DNS Records for correct entries.

2. **Problem:** User is repeatedly prompted for their password?

Cause: Old credentials are cached.

Fix: Remove old profile and/or clear old cached credentials.

3. **Problem:** Why are my e-mails being tagged as SPAM?

Cause: SPF/DKIM does not match.

Fix: Correct the SPF/DKIM DNS Authentication Records for Domain.

4. **Problem:** Where are historical e-mails?

Cause: Archive was not migrated.

Fix: Restore archive from back-up or PST.

30-Day Implementation Checklist

Days 1–10: Preparation

- Audit users/mailboxes.
- Verify that you have access to DNS control.
- Export any important mailboxes.
- Confirm compliance with the GDPR.
- Create a plan for migration.

Days 11–20: Migration

- Create a new tenant.
- Establish a baseline for security.
- Migrate test users.
- Migrate all other mailboxes.
- Schedule a time to cutover the DNS.

Days 21–30: Stabilisation

- Verify that all mail is flowing.
- Train employees how to use their new mail.
- Disable access to the old system.
- Audit administrator permissions.
- Document the final state of the new infrastructure.

FAQs

1. Will emails be lost in the migration?

As long as the migration is fully planned and has proper backups, no emails will be lost.

2. What is the average time to complete the migration?

For ten users, it typically takes one to three days; for 30 users, (1 week with the possible addition of time for testing).

3. Is it best to migrate overnight or during the day?

Ideally, the cutover should occur during times of low activity.

4. Can staff continue to use email during the migration?

Typically yes, until the DNS cutover.

5. Do we need a backup of all our emails even though we are using Microsoft 365?

Yes, because Microsoft only provides a 99% availability service, not a full data service.

6. What is DNS propagation?

The amount of time that it takes to propagate/complete a change in the MX record throughout the world.

7. Is migration a high-risk process?

There is little risk in a structured plan; however, High-risk exists when migration is rushed.

8. Is IT support helpful for this migration?

Yes: IT support is essential in regard to the DNS and security set up for the new hosted environment.

9. What happens to the existing mail server?

It will be kept accessible for a brief time period after cutover but will eventually be securely decommissioned.

10. Will a successful email migration increase email security?

A successful migration can lead to more secure emails as long as two-factor, modern security-supported technology is in place.

11. Are shared user mailboxes difficult to set up?

Shared user mailboxes are only complicated if there is no standard format in the documentation.

12. Should I notify my clients about the migration?

Generally no, unless there will be any downtime or service interruptions due to the migration.

About This Guide

Computer Support Centre (http://www.computersupportcentre.co.uk) is a UK-based IT consultancy who specialise in supporting SMEs. We have produced this guide based on our experience of supporting UK offices in planning and implementing secure email migrations without disruption.

The recommendations in this guide are based on lessons learned through our work with UK companies with 1–50 employees and are focused on the following: effective planning, data security, improving security, and minimisation of downtime, and not adding to the confusing complexity of technology.

The recommendations in this guide have been developed in keeping with UK best practice, including but not limited to the aspects of UK GDPR and the regulatory expectations set by the Information Commissioner’s Office (ICO). We have specifically designed our recommendations to assist non-technical managers to undertake the necessary investigations and make well-informed decisions with confidence.

At **Computer Support Centre,** our vision is simple: to provide straightforward, low-cost and actionable advice that enables UK businesses to have a secure and efficient future.

Conclusion

Migrating email systems from one software to another is not a stressful and risky process if prepared adequately with careful planning, audit checklists, and robust security measures. UK small to medium businesses (SME's) can migrate to a current email platform confidently and without complications if they adopt a well-thought-out plan for migration focused on preparing well in advance of the actual email platform put into production. Prepare first by backing up any existing email data, securing accounts being migrated, managing DNS correctly, and testing thoroughly all components of new software and hardware solutions before shutting down old systems. A systematic methodology will protect your business as well as your employees and customers during the email migration process.