MICROSOFT 365 SETUP GUIDE FOR UK SMES

A practical, security-first setup guide for UK small and medium businesses

For UK businesses with 5–200 users

✓ *Security-first Microsoft 365 setup*
✓ *UK GDPR & governance aware*
✓ *Practical checklists & rollout plan*

Prepared by:

© Computer Support Centre

Microsoft 365 Setup Guide for UK SMEs (2026)

Executive Summary

- Microsoft 365 is the standard item for small to medium-sized enterprises in the UK; Unfortunately, without an appropriate configuration, Microsoft 365 can create significant risks to the security and compliance of an organisation.
- To avoid typical pitfalls like mismatched licensing or neglected data sources, start with planning and prerequisites.
- Written for non-technical decision-makers, this guide also provides practical information that can be followed by the administrators responsible for implementing this work.
- Put security first: To prevent phishing and security breaches, enable MFA, Conditional Access, and endpoint basics.
- The guide contains a very brief overview of GDPR and compliance, while purposefully avoiding making claims.
- Add migration checklists from file sources with zero-downtime advice, on-premise Exchange, or Google Workspace.
- For quick wins, use the Fast Track (Day 1) checklist; for a full rollout, use the 30-day plan.

Who This Guide Is For

This guide was created specifically for UK small and medium-sized enterprises (SMEs) with between 5-200 employees, including:

- Business owners and directors
- Operations/office managers
- IT coordinators/junior administrators
- Organisations moving from older technology platforms, such as Google Workspace, legacy e-mail accounts and on-premises systems
- Junior admins tasked with implementation

No specialist IT experience is required in order to use this guide.

What You'll Achieve

The key benefits of using this guide are as follows

- Create a clean and well-designed Microsoft 365 tenant
- Lower exposure to security threats with sensible defaults
- Clear decision making with respect to licensing/configuration
- Roll out email, Teams, and file storage correctly
- Increased redundancy due to Backups & Audit logs
- Avoid common mistakes that cause long-term pain

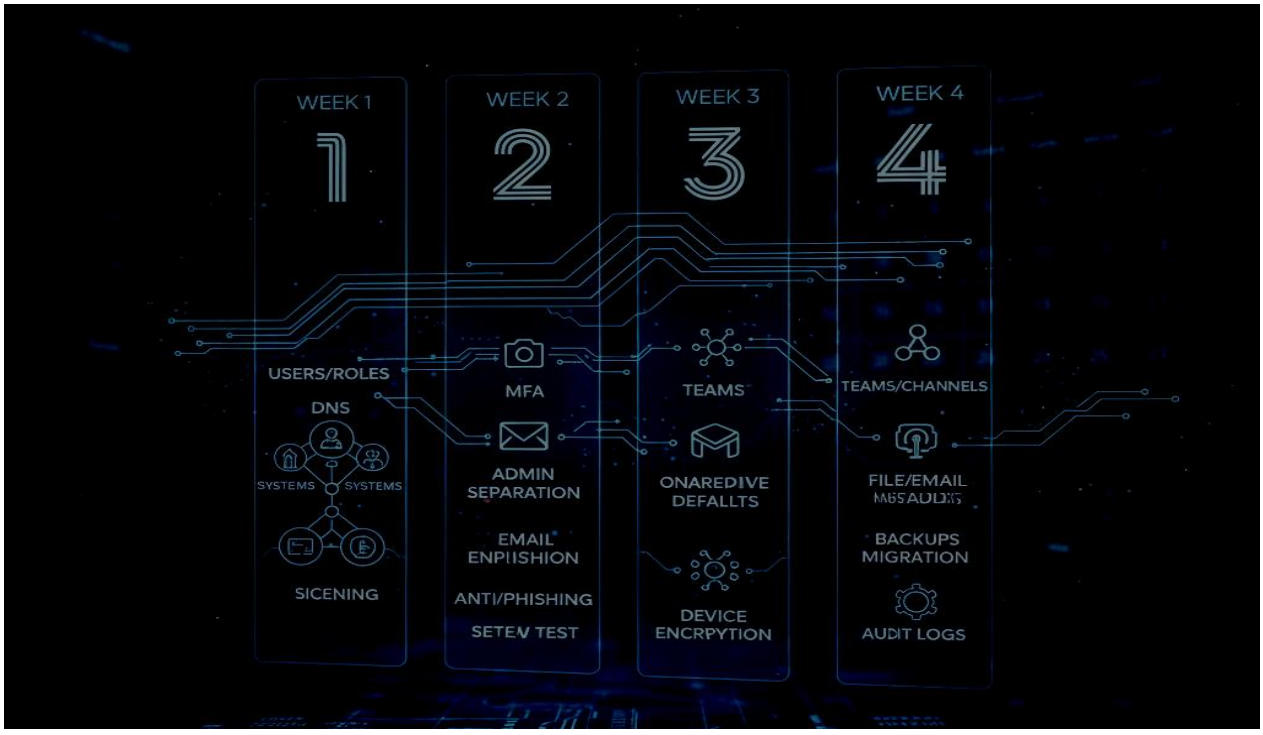
Fast Track: Day 1 Checklist

1. Use this list if you need to quickly establish your safe baseline.
2. Create your first User Accounts
3. Implement a Strong Password Policy
4. Create a new Microsoft 365 Tenant
5. Verify your Business Domain and add it to the Tenant
6. Create a new separate Admin Account, which is different from the one used daily
7. All Admin accounts need to enable MFA (Multi-Factor Authentication)
8. Choose licences (Basic / Standard / Premium)
9. Enable Audit Logging
10. Setup Basic Conditional Access for Administrators
11. Set Default Sharing Restrictions
12. Disable Legacy Authentication
13. Create Shared Mailboxes
14. Set Default Exchange Spam and Phishing settings
15. Create Teams Meeting Policies
16. Confirm Device Encryption Status
17. Restrict External Sharing by Default
18. Enable Microsoft Defender by Default
19. Confirm that OneDrive is Enabled
20. Enable Retention by Defaults
21. Document who has Admin Access to the Tenant
22. Schedule a Migration Window
23. Inform All Users about the Implementation of MFA

24.

Standard Setup Plan (30 Days)

Week 1: Foundations & Planning	**Week 2: Security, Email, and Identity**
1. Verify DNS and domain access 2. Make a list of users and roles 3. Examine the current file and email systems. 4. Make a licensing decision 5. Establish base and tenant settings	1. Implement MFA for every user. 2. Keep user and admin accounts apart. 3. Set up email authentication. 4. Implement anti-phishing measures 5. Test the mail flow
Week 3: Devices & Cooperation	**Week 4: Data, Backups, and Compliance**
1. Design Teams and channels 2. Establish a SharePoint framework 3. Set up the OneDrive defaults 4. Turn on device encryption	1. Transfer files and emails 2. Turn on backups 3. Set up retention 4. Examine the audit logs



1) Planning & Prerequisites

Gather the following before you begin utilizing Microsoft 365:

Access and Information

1. Domain Registrar Login
2. DNS Access
3. Users and Roles List

4. Current Email Provider
5. Where Files are Stored
6. Devices (e.g. Windows PC, Mac, Mobile)

Naming Convention

1. All Usernames (i.e., Firstname.lastname@companydomain.co.uk)
2. Any Shared...Mailboxes (i.e., info@, support@, accounts@)
3. Any Teams (Departments – Functions)
4. Any SharePoint Sites (Departments or Purposes)

Shared Mailboxes & Groups

1. Use Shared Mailboxes for roles not people
2. Use Distribution Groups for Announcements
3. Use caution with Nested Groups early on

2) Microsoft 365 Licensing (UK SME Guide)

Business Basic...Choose if:

1. Only Email + Web...Apps required
2. Minimal Security Required
3. No Device Management Required

Business Standard...Choose if:

- Desktop Office Apps Required
- Teams and SharePoint are core applications
- Acceptable Level of Light Security

Business Premium (Recommended for most SMEs)...Choose if:

- You want a high security level
- You want to manage devices
- If you have remote or hybrid employees
- If compliance and control is important

General Rule of Thumb:

- If Security is Important to you in any way, Business Premium will likely pay off.

3) Setting Up a Tenant

Step by Step Instructions:

- Create tenant at Microsoft 365 admin portal

- Enter your organisation’s name and location.
- Add and verify your own domain.
- Determine your organisation’s default language and time zone.
- Create a Microsoft 365 administrator account.
- Add the required licenses for your organisation to use Microsoft 365.
- Confirm that security settings match your organisation’s baseline.

4) Identity & Access

What is MFA?

MFA (multi-factor authentication) requires an additional verification step via SMS or app.

Why is MFA Important?

MFA stops the majority of hackers.

Recommand Approach:

- Enforce MFA for All Employees
- Use app-based authentication
- Do Not Allow Exceptions for Admins

Admin Accounts

- There Should Only Be One Admin Account for Each Employee.
- Admin Accounts Should Not Be Used for Daily Email Activity.
- Use the Least Privileged Role Possible for Admins.

Starter Policies?

- MFA Is Required for Admin Accounts
- Block All Legacy Authentication
- A Compliant Device Is Required to Access Your Admin Account.

5) Email Setup

What Is Email Authentication? (You Must Do This)

- MX record is used to route email to Microsoft Exchange (MX).
- SPF record is used to authorise senders to send emails.
- DKIM record is used to prove that email messages have not been tampered with in transit.
- DMARC record is used to control whether or not other servers can send email on behalf of your company.

- Email Authentication Is Critical to Protecting Your Brand Reputation and Reducing Phishing Attacks.

What Are Some Quick Wins to Prevent Phishing Attacks?

- Enable Impersonation Protection on Your Domain
- Protect the Name of Your Domain
- Enable Safe Links and Attachments.

6) Teams and Collaboration

Teams Structure

- Each Department Should Have a Separate Microsoft Team;
- Each Team Should Have Channels Based on Topics, Not Departments.
- Avoid creating teams for every chat

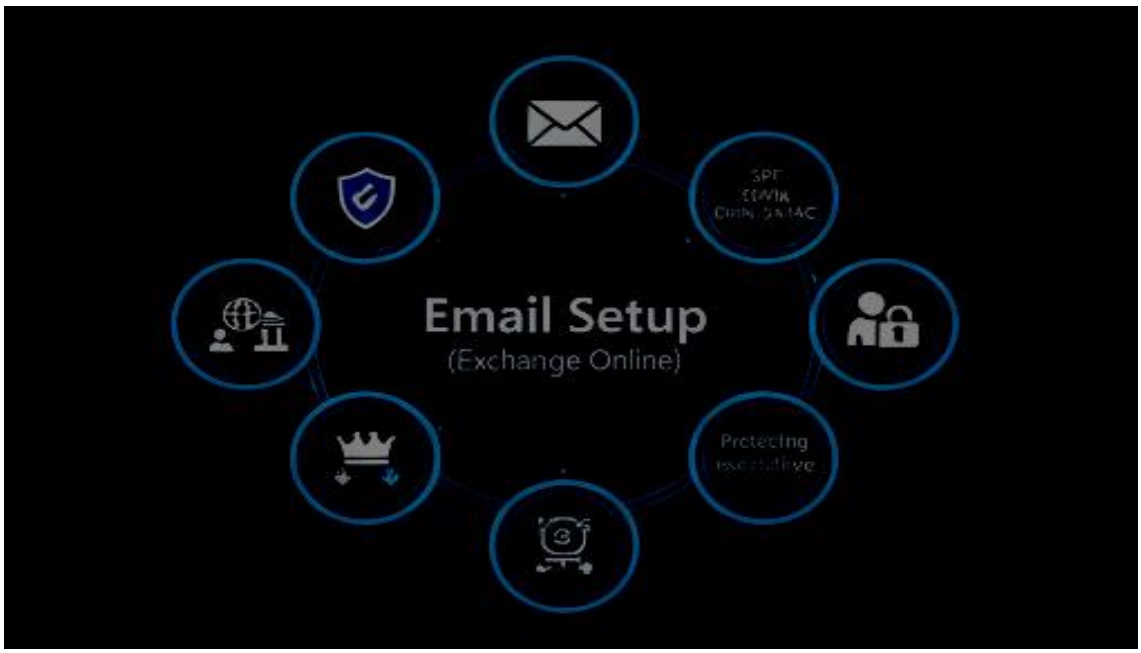
External Access

- Default: Disabled
- Allow only when needed
- Quarterly Review

7) SharePoint and OneDrive

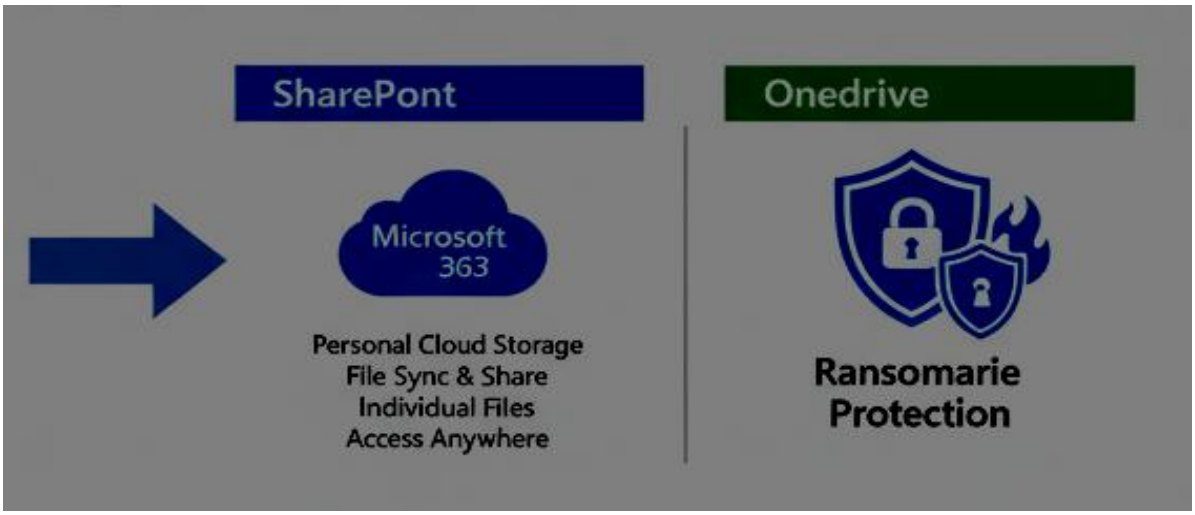
Where to store what

Use Case	Tool
Personal Work Files	OneDrive
Team Documents	SharePoint
Departmental Data	SharePoint
External Sharing	SharePoint-Controlled



Permissions

- Use Groups instead of Individuals
- Simplicity should rule the day
- Review permissions regularly



8) Device Security & Management

Basics

- Bit-locker should be enabled on all Windows systems
- FileVault should be enabled on all Macs
- All OS Updates should occur automatically
- Have Microsoft Defender enabled

Intune (Business Premium)

- Require Compliance for all devices
- Enforce Encryption on all devices
- All apps should have Basic app protection policies

9) Backup & Continuity

Why Backups are Necessary?

- Because Microsoft 365 is not a complete backup solution

Why do we need Backup?

- Accidental deletions
- Ransomware
- Retention gaps occur

Types of backups

- Third-party Microsoft 365 Backup tools
- Cloud-to-cloud backups
- Daily automated backups

10) GDPR & Compliance (High Level)

- Data is stored in Microsoft UK/EU Data Center.
- Retention Policies are in place to protect records.
- eDiscovery supports investigations.
- Audit Logs track all actions taken by users

This information is not Legal advice be mind it.

Security Baseline (Recommended Defaults)

Setting	Recommended Default	Why	Where
MFA	Enable for all users	Prevents breaches	Entra ID
Anti-phishing	Enable safe links/attachments	Scans email for threads	Security admin centre > Email & collab > Policies
Admin roles	Separate accounts	Least privilege	Admin centre
Legacy auth	Disabled	Blocks old attacks	Entra ID
DKIM	Enabled	Email trust	Exchange
Audits log	Enabled	Investigation	Compliance
Sharing	Restricted	Data control	SharePoint

Typical UK SME Scenarios

A) 10 User Professional Service Company with a premium license focusing on Microsoft Teams and email, Moving from Google to Microsoft.

B) 30 User Retail/Back Office with a minimally functional standard license with Premium Licensing for devices, built out SharePoint to manage inventory, and migrate to Microsoft from Dropbox.

C) 100 User Mixed Remote / Office 100% Premium Mandatory, Intune compliance, Conditional Access based on geography. Hybrid rollout from exchange server to Exchange Online.

Go Live Checklist

- Final Data Sync
- DNS Update (MX/SPF)
- Notify Users (Outage Window)
- Access / Email Testing
- Queue Monitoring

Post Go Live Checklist (First 30 Days)

- Gather user feedback
- Conduct Secure Score Scan
- Conduct Backup Testing
- Conduct Audit Log Review
- Train on New Features
- Optimization of Policies

Common Mistakes (Top 15)

- Mostly Skipping MFA
- You only have one admin account that is shared among all users
- Not backing up your data
- You do not have a system to handle naming your files
- Do not review your audit log regularly
- Do not provide training for your users
- Using weak authentication on your email
- Not encrypting your devices
- Using personal email accounts for work purposes
- Do not have documentation of your user accounts

- You have adopted a "set it and forget it" mentality

FAQs

What is the best M365 plan to use for an SME In the UK?

✓ The Premium Plan (16.90 per user per month) is ideal for providing enhanced security, while Standard Plan (9.60 per user per month) is appropriate if you are only using basic applications.

Is M365 compliant with GDPR for UK-based businesses?

✓ M365 provides tools, including Purview and residency, to help you comply with GDPR. However, you are ultimately responsible for how your M365 account is configured for GDPR compliance. Therefore, M365 does not provide a legal guarantee regarding GDPR compliance.

How can I enable Multi-Factor Authentication (MFA) in M365?

✓ To enable MFA in M365, navigate to your Entra Admin Centre under MFA, and then click the "Enable" button for MFA.

What is Conditional Access?

✓ Conditional Access is a set of policies that define the conditions under which users are allowed to access your M365 account.

What is the difference between SharePoint and OneDrive?

✓ SharePoint is designed for use by teams (Collaboration) and OneDrive is designed for personal use (Personal Storage)

Can I use Intune to manage mobile devices?

✓ Yes, you can use the Intune app to enrol your mobile devices into M365 to ensure compliance with your organisation's security policies.

About This Guide

The **Computer Support Centre** has produced this Microsoft 365 Setup Guide to assist UK small and medium-sized enterprises in implementing Microsoft 365 in a structured, secure, and implementable manner.

The guide is based on our professional experiences working with organisations using Microsoft 365 on a day-to-day basis, including the use of email, collaboration tools, identity and access management, device protection, and compliance.

Unlike many guides that focus on the technology alone, our planning guide focuses on the procedures, processes, best security defaults, and long-term management of your Microsoft 365 implementation so that your organisation can continue to grow in confidence and have complete control over your IT system.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

When it is set improperly, Microsoft 365 can cause many problems for UK small and medium-sized enterprises. Using a systematic, security-based setup will yield positive results for organisations by avoiding common errors, lowering the potential for risk, and establishing a stable base of operations for everyday activities.

Following this setup guide will enable an organisation to implement Microsoft 365 efficiently, reliably, and effectively. Rather than relying on “quick-fix” philosophies, this guide places emphasis on the tools, processes, best security practices, and long-term management of the product.