Employee IT Onboarding Checklist

Why IT Onboarding Matters for UK Businesses

The **first week** of work can **create a strong foundation for new employees** to embrace your company's culture; however, they will struggle to become productive members of the business if their IT onboarding is not planned accordingly and they do not have easy access to the tools and applications they need to be productive.

Small to medium-sized enterprises (SME) within the UK often carry out their IT onboarding with little structure. For example, an office manager may quickly set up all of the accounts a new employee will require to do their job, a laptop will be ordered for them, and the passwords are often shared quickly so the employee can begin work.

While this may seem like a good way to think about onboarding new team members, this type of process creates multiple operational and security challenges.

With little structure in place for IT onboarding, an SME may face a variety of challenges, such as:

- Sensitive information being shared with the wrong employee.
- New employees using their personal emails to conduct work-related communications.
- Employees using weak passwords to access their accounts, placing both the employee and the organisation at risk.
- Missing laptops or tracking of IT equipment.
- Delayed response times for new employees to be set up and working with their team.

Creating a structured IT onboarding process ensures that new employees are provided with the equipment necessary to perform their job while protecting the data and systems of the organisation.

It also provides an organisation with the ability to control access to information, thereby assisting with meeting basic data-protection requirements.

What IT Onboarding Includes

IT onboarding for employees is all the substantiation people need to give a new worker secure and dependable access to company systems.

In most cases, for SMEs, IT onboarding would involve the following:

- Setting Up Company Email Account
- Access to file sharing via company network
- Company provided laptop/desktop preparation
- Installation of all required software
- Access to company collaboration tools
- Setting Password Policy
- Multi-Factor Authentication enabled
- Providing security guidance

- Documenting company assets

Typically, IT onboarding involves the collaboration of HR, manager, and person managing the technology to the company.

Properly organising these steps will facilitate quicker and secure employee onboarding and working less time.

Common Mistakes Businesses Make When Onboarding Employees

SMEs often inadvertently expose themselves to risks when it comes to onboarding because they have informal or inconsistent onboarding processes.

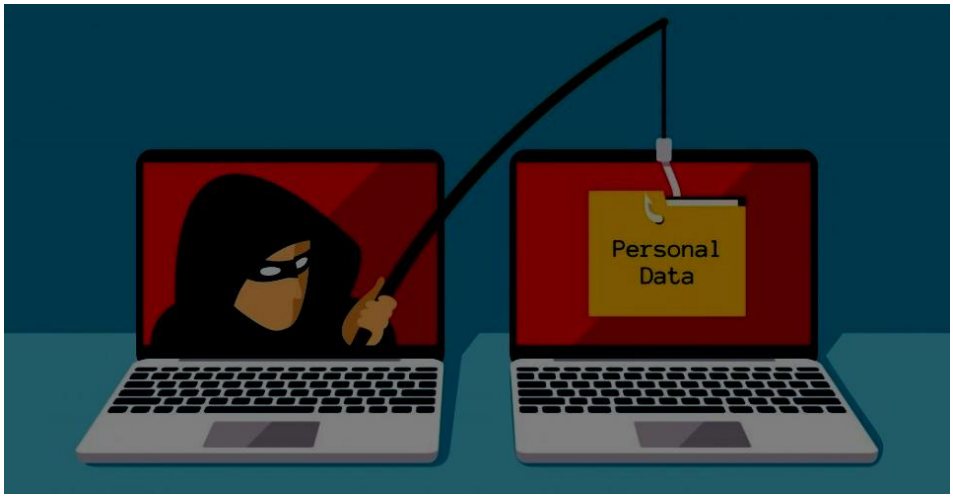
Examples of common mistakes are:

No Laptop On Day One

When employees show up ready to work, there is often a several-day wait for their device to be configured.

Personal Email Use

When business email is not ready, an employee may use their personal email account for work communications.



Too Much Access to Files

New users may gain access to entire drives instead of just the files they require.

Password Sharing

Sharing passwords, although offered for convenience, decreases security.

Absence of Multi-Factor Authentication

If only a normal login is needed to log into an account, it makes it easy for someone who has compromised your password to access your information.

No Device Tracking

A company can easily lose track of laptops or mobile devices assigned to its employees.

While these may not seem like major mistakes, they can lead to lost productivity or expose your data.

Pre-Start IT Preparation

The most successful employee onboarding begins before they set foot in the company, with many of the IT preparations being completed so that they can begin their roles on day one.

When IT systems are ready in advance, new starters have everything they need to be able to start working immediately.

The following tasks are typically completed as part of the pre-start IT preparation:

- Creation of the employee's company email account
- Assignment of collaboration tool licenses (e.g., Microsoft Teams, Slack, etc.)
- Preparation of employee laptop/desktop
- Installation of necessary software
- Access permission set up for folders/files
- Recording devices in asset register
- Provision of employee with instructions for accessing their logins

When pre-start activity has been conducted in advance, day one for all parties is greatly improved.

First-Day IT Setup

On the first working day of an employee, the focus is on testing that everything works correctly.

The following tasks are typically completed as part of the first-day IT “Set-Up”:

- Provision of the employee's laptop/desktop
- Verification that the employee's login credentials work
- Test email access
- Access necessary shared files/systems
- Introduce to the collaboration tool set
- Explain basic security
- Provide IT support contact details

If pre-start work has been completed correctly, then the initial set-up process will typically take less than one hour to complete.

Access and Account Setup

Creating An Email Account

It is required that every employee have a company email account.

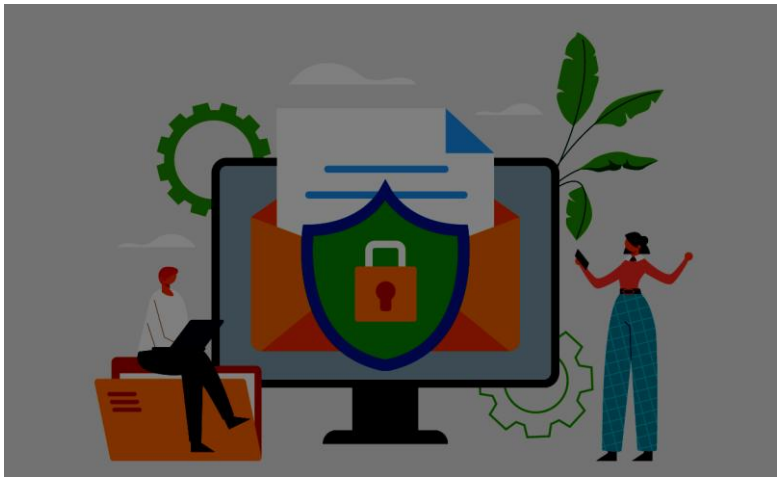
Typically, companies use the following platforms:

- Microsoft 365,
- Google Workspace

Best practices for email account creation are:

- Maintain consistency in naming conventions for email accounts.
- Use a secure password.
- Limit access to your email mailbox to individuals outside of your organisation.

Employees should never use their personal email account to communicate on behalf of the organisation.



File Access

Access to files should be given to each employee based on the access required for their role using the least privilege principle.

For example:

- HR will only have access to HR files
- Finance will only have access to finance-related data
- Marketing will only have access to marketing files

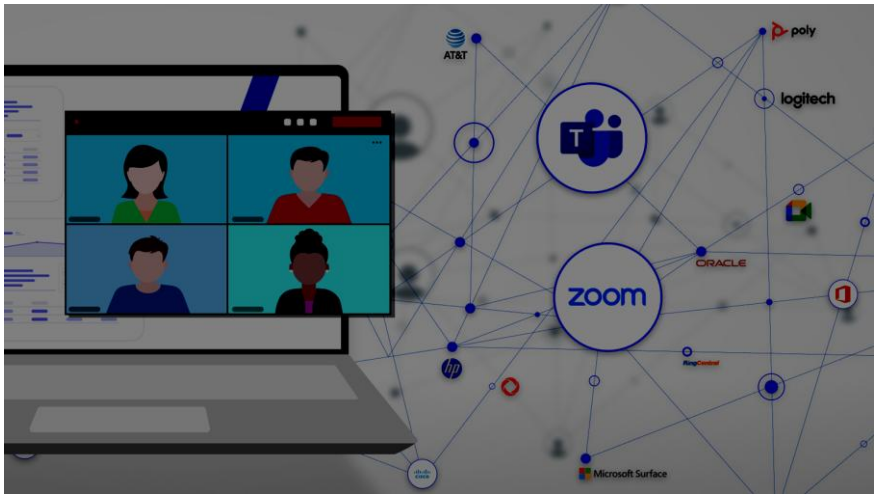
This reduces the risk of inadvertently exposing sensitive data.

Collaboration Tools Access

The majority of small to medium-sized enterprises (SMEs) will use digital tools to assist with collaboration, such as:

- Microsoft Teams,
- Slack,
- various project management tools.

Access to digital collaboration tools should follow from the employee's department and job responsibilities.



Security measures for new employees

Password Security

All businesses should enforce strong password policies.

Key points of password policy include:

- Minimum password length requirements
- Avoidance of using commonly used words as passwords
- Not reusing the same password for more than one account

A password manager can be a recommended solution for employees to manage their complex passwords in a secure manner.

Multi Factor Authentication (MFA)

MFA provides another additional layer of security protection.

If an attacker steals a user’s password, they can not easily access the user's account without the second factor used for verification.

MFA can be found within many email and cloud-based platforms that provide mobile device-based authentication apps.

Security Awareness Training

New employees should receive basic security awareness training including:

- How to identify phishing emails
- How to protect sensitive data
- How to lock their computers when leaving them unattended
- How to report any suspicious activity

Even a brief security awareness course may have a significant impact on the overall amount of risk associated with a business's cyber security.

Considerations for Onboarding Remote Workers

In the UK, it is now quite prevalent for companies to have both remote and hybrid employees.

This necessitates a larger set of considerations for onboarding.

Remote Employees

- Remote employees may receive their devices via courier, and ideally, the company will set up the remote employee to confirm that everything works before they start.

Hybrid Employees

- Hybrid employees need to have access to the same resources at home and in the office.
- The systems will allow employees to securely log in from both locations.

Secure Home Office Setups.

When working from home employees should follow a few simple guidelines:

- Connect to a secure Wi-Fi network.
- Do not use public Wi-Fi networks for any work that is sensitive.
- Make sure that their devices will be secure.

Remote Device Management

Companies will be able to use their remote management tools to:

- Deploy software updates.
- Check the health of their remote devices.
- And, to help secure lost devices.

Thus, remote employees' devices will be protected.

Complete Employee IT Onboarding Checklist

Pre-Start Checklist	First-Day IT Setup Checklist
❿ Create email account ❿ Software licence assignments ❿ Setting up of hardware. ❿ Creating & installing the required applications. ❿ Setting the correct security settings. ❿ Providing access to needed files for employee's first day. ❿ Adding employee to the collaboration application. ❿ Recording employee's device in an asset register.	❿ Provide device to employee ❿ Confirm login credentials ❿ Test email access ❿ Confirm file access ❿ Introduce collaboration tools ❿ Provide IT support contact

FAQs

1. What does IT onboarding entail?

Creating accounts, setting up devices, installing software, granting access permits, and configuring security.

2. How long does it typically take to onboard an employee through IT?

Onboarding could take roughly an hour to an hour and a half for the employee to complete their first-day responsibilities provided that proper planning has been done ahead of time.

3. Who is responsible for onboarding employees through IT?

Typically, community members include both IT support and/or any external IT providers who collaborate with either HR staff or the office manager.

4. What actions can an organisation take to ensure new employee accounts are secure?

An organisation will need to establish/enforce strong password conditions, enable Multi-factor Authentication on accounts, apply Role-based Access Control to systems, and limit the number of employees with access to sensitive information.

5. What tools are available for organisations to use when managing employee IT set-up?

There are several types of tools available for managing an employees' IT setup. These are generally related to specific software programs and may include Microsoft 365 Administrator Tools, Device Management platforms, and Password Managers.

About This Guide

Computer Support Centre wrote this guide to assist small and medium-sized enterprises (SMEs) in the United Kingdom with creating a clear and secure IT onboarding process for their new employees. Many companies are able to set up employee accounts, devices and access rights very quickly, however, if there is no established procedure in place, then those accounts, devices and access rights

could also be set up incorrectly, which will present serious security risks to the organisation, frustrate the new employee and delay productivity.

The objective of this guide is to outline the major milestones in the IT onboarding process of new employees by detailing the process of preparing devices before the employee's start date, providing system and email access, establishing security measures, and ensuring safe employment for remote or hybrid employees. Utilising a formalised IT Onboarding process can lead to faster onboarding of new employees while ensuring the continued protection of the organisation's systems and data in the process.

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

 https://computersupportcentre.com

Conclusion

To successfully onboard new hires into your organisation, you'll need to create an IT on boarding plan that will allow new employees to assume their roles in an efficient and secure manner. If new employees can be granted access to their business accounts, devices, and permissions before starting their jobs, they will be able to devote all of their attention to completing their tasks with minimal technical issues in their first few days at work.

Establishing strong security policies such as implementing strict password requirements, enabling multi-factor authentication and restricting access to files allows companies to better secure sensitive information while ensuring that their IT infrastructure is well-organised. In addition, properly documenting IT inventory and tracking all IT assets helps companies properly manage their technology as they continue to grow.

By developing a standardised, comprehensive information technology onboarding checklist, UK small to medium sized enterprises can improve employee productivity, improve data security and help provide a better overall experience for each new employee that joins the organisation.