REPEATABLE PROCESS

Starters & Leavers

Two checklists you can use every time, so a new starter works on day one and a leaver's access closes the day they go.

Almost every business does this from memory, and almost every business gets it wrong occasionally — a new starter waiting three days for a mailbox, or an account still active six months after someone left. Neither is a technical problem. Both are the absence of a written list.

These two pages are that list. Print one per person, work down it, keep it on file. It is deliberately dull, and that is the entire value: the same steps, every time, regardless of who is doing it or how busy the week is.

WHY IT IS WORTH THE TEN MINUTES

A starter who works on day one

First impressions of an employer are formed in the first hours. Someone sitting unable to log in learns something about how the business runs.

A leaver who is genuinely gone

Active accounts belonging to former staff are a real security exposure, and one of the most common findings in any audit.

Licences you stop paying for

Unremoved licences are among the most common wasted costs in an SME — and the easiest to recover once someone checks.

Work that does not leave with them

Files, mailbox contents and half-finished jobs handed over deliberately rather than discovered missing weeks later.

ONE RULE WORTH ADOPTING

Nothing on the leaver list waits for "when we get a moment". Access closes on the last day — ideally at the hour they finish. Everything else on that page can follow at a sensible pace.

THIS IS A SHARED PROCESS, NOT AN IT ONE

Whoever handles IT cannot remove access they do not know exists, and cannot prepare for a starter nobody told them about. Managers notifying IT promptly — ideally at the point of offer or resignation rather than the week itself — is what makes either list work.

CHECKLIST ONE

New Starter

NAME _____ ROLE _____ START DATE _____

BEFORE THEIR FIRST DAY

	TASK	WHEN	DONE BY
☐	**Create their account** One account per person, in their own name. Never reuse a leaver's.	WEEK BEFORE	
☐	**Assign the right licence** Match the plan to the role rather than copying whoever sits nearest.	WEEK BEFORE	
☐	**Set up multi-factor authentication** Enrolled on day one, before habits form. Authenticator app rather than texts.	DAY ONE	
☐	**Register a security key or passkey if you use them** Where the business has adopted phishing-resistant sign-in, enrol them at the same time as MFA.	DAY ONE	
☐	**Add to the right groups and Teams** Access by group, not person — it is far easier to review and to revoke.	WEEK BEFORE	
☐	**Prepare and assign the device** Standard build, encrypted, updated, and recorded against their name.	WEEK BEFORE	
☐	**Install the software they actually need** Including any line-of-business system, with its own account created.	WEEK BEFORE	
☐	**Set up phone or mobile access if required** Work email on a personal phone still needs to be a deliberate decision.	WEEK BEFORE	
☐	**Add to shared mailboxes and distribution lists** info@, sales@, the team calendar — the things nobody remembers until day three.	DAY ONE	

FIRST DAY AND FIRST WEEK

☐	**Walk them through where files live** Mine versus the business's. Ten minutes now saves months of files on desktops.	DAY ONE	
☐	**Show links, not attachments** The single habit worth teaching on day one, while nothing is ingrained.	DAY ONE	
☐	**Give them the security basics** Phishing, verifying payment requests, and who to tell if something looks wrong.	WEEK ONE	
☐	**Set up a password manager** For the twenty non-Microsoft accounts the business also uses.	WEEK ONE	
☐	**Tell them who to contact for IT problems** One route, written down. Obvious, and routinely missing.	DAY ONE	
☐	**Check in after a week** Five minutes. Most access gaps surface here rather than on day one.	WEEK ONE	

> **IF THIS LIST TAKES A LONG TIME**
>
> That is worth noticing. A well-set-up environment lets most of this happen in under an hour, largely automatically. If it routinely takes a day, the process is doing work that configuration should be doing.

CHECKLIST TWO

Leaver

NAME _____ ROLE _____ LAST DAY _____

ON THEIR LAST DAY — NOT AFTER

	TASK	WHEN	DONE BY
☐	**Disable the account — do not delete it** Blocks access immediately while keeping their data recoverable and handover-able.	LAST DAY	
☐	**Sign them out everywhere** Revoke active sessions. Disabling an account does not always end a logged-in session.	LAST DAY	
☐	**Remove remote and VPN access** Including anything a supplier or third-party tool grants separately.	LAST DAY	
☐	**Remove them from third-party systems** Accounts package, CRM, job system, social media, banking. The list nobody keeps — keep one.	LAST DAY	
☐	**Collect equipment** Laptop, phone, access card, keys, any hardware token. Tick when received and record any missing items — a note now is far easier than a conversation months later.	LAST DAY	
☐	**Remove any registered keys or passkeys** Security keys, authenticator registrations and any device still trusted for sign-in.	LAST DAY	
☐	**Change any shared credentials they knew** Especially if passwords were ever shared informally rather than through a manager.	LAST DAY	

WITHIN THE FIRST WEEK AFTER

☐	**Hand over their files** Move business content out of their OneDrive to where the team can reach it.	WEEK ONE	
☐	**Decide what happens to their mailbox** Convert to a shared mailbox, or forward to a colleague for an agreed period.	WEEK ONE	
☐	**Set an out-of-office or redirect** So clients and suppliers are not left emailing into silence.	LAST DAY	
☐	**Reassign their work and responsibilities** Open jobs, approvals they owned, systems only they administered.	WEEK ONE	
☐	**Remove or reassign the licence** Only once the mailbox and files are dealt with — then stop paying for it.	WEEK 2–4	
☐	**Remove them from the device record** Reset and reissue the laptop, and update your inventory.	WEEK 2–4	
☐	**Note anything only they knew how to do** Before the knowledge is gone. This is the step most often skipped and most often regretted.	BEFORE THEY GO	

ROLE CHANGES COUNT TOO

When someone moves internally they usually gain access and rarely lose any. Run the relevant parts of both lists — add what the new role needs, remove what the old one did. This is how permissions quietly sprawl over years.