Bring Your Own Device (BYOD) Policy

Policy · UK · Updated 2026-07-23 · Square brackets are placeholders to replace with your own details.

A bring your own device (BYOD) policy sets the rules for staff using personal phones, tablets, and laptops for work — which devices are allowed, the security they must have, what the employer can and cannot see or wipe, and what happens when a device is lost or its owner leaves. It draws the line between company data and private life on the same piece of hardware.

BYOD happens whether or not you write it down: the rota checked on a personal phone, the customer email answered from a home laptop. The choice is not whether staff use their own devices but whether the risk is managed — an unmanaged personal device holding work data is one of the commonest ways small businesses lose control of personal data.

This template covers approval and eligible devices, security requirements, working rules, privacy boundaries, loss and leaver procedures, and costs — the full text below is a worked example you can adapt line by line.

Purpose and scope

This policy applies to anyone using a personal device — phone, tablet, or laptop — to access [Your company] systems or data, including email, [messaging platform], [rota/CRM system], and work files. Using a personal device for work is optional for staff, and conditional on this policy for the company.

It protects two things at once: company and customer data on devices we do not own, and the private lives of the people who own them.

Policy statement

Personal devices may be used for work only with approval, only through [approved apps/access method], and only while the security requirements below are met. [Your company] may withdraw access at any time. We will never browse the personal content of your device.

Approval and eligible devices

Ask [name/role] before connecting a personal device to any work system. Approvals are recorded in the [BYOD register] with the device type and what it may access. Devices that no longer receive manufacturer security updates are not eligible. Roles handling [sensitive data categories — e.g. health or financial records] are excluded from BYOD and use company devices instead: [list roles].

Security requirements

- Protect the device with a PIN, password, or biometric lock that engages automatically.
- Keep the operating system and apps updated — stop using any device that no longer receives security updates.
- Turn on device encryption where it is not already on by default.

- Do not use a jailbroken or rooted device (one with its built-in security removed) for work.
- Install [mobile device management / approved security app] if we require it for your level of access.

Working on your own device

- Access work systems only through [approved apps — e.g. the company email app or browser portal]; never forward work email to personal accounts.
- Keep work files in [company cloud system], not in the device's local storage or personal cloud accounts.
- Do not let family members or anyone else use the device while you are signed in to work systems.
- Avoid public Wi-Fi for work, or use [VPN/approved method] when you have no alternative.
- Do not photograph anything containing customer or staff personal data unless a work process specifically requires it.

Your privacy — what we can and cannot see

[Your company] can see and manage the work side only: [describe — work accounts, the contents of approved work apps, access logs]. We cannot and will not look at your personal photos, messages, browsing history, or location.

If we use remote wipe, it is limited to work data and work apps wherever the technology allows. A full-device wipe is a last resort for a lost device that cannot be selectively wiped, and we will tell you before triggering one unless delay would materially increase the risk.

Lost devices, incidents and leavers

1. Report a lost or stolen device with work access to [name/role] immediately, at any hour.
2. [Name/role] revokes the device's access to work systems and triggers remote wipe of work data where enabled.
3. If personal data may be exposed, follow the data breach response procedure — the 72-hour ICO clock runs from awareness.
4. When you leave [Your company] or stop using BYOD, work accounts and data are removed from your device on or before your last day, and you confirm in writing that none remains.

Costs, support, records and review

[State your position: [Your company] contributes [amount] per month for approved regular users / work calls and data are reimbursed through the expenses policy / no contribution is made for optional BYOD.] IT support covers the work apps and connections only — we do not repair or maintain the device itself.

The BYOD register, approvals, and signed acknowledgments are kept in [system/location]. This policy is reviewed [frequency] and whenever the systems staff can access change. Owner: [name/role]. Next review: [date].

How to use this template

1. Decide first which systems personal devices may reach — the narrower the access, the simpler everything else becomes.
2. Test your remote-wipe capability on a spare device before you rely on it in the lost-device procedure.
3. Write the privacy section with whoever runs your IT, and describe only what your tools actually do — accuracy in both directions.
4. Choose your costs position and put it in writing; unspoken expectations about personal data allowances breed resentment.
5. Get a signed acknowledgment before enabling access, not after.
6. Add the device step to your leaver checklist so it happens on the last day, every time.

Official guidance

- ICO — UK GDPR guidance and resources
- ICO — Report a breach