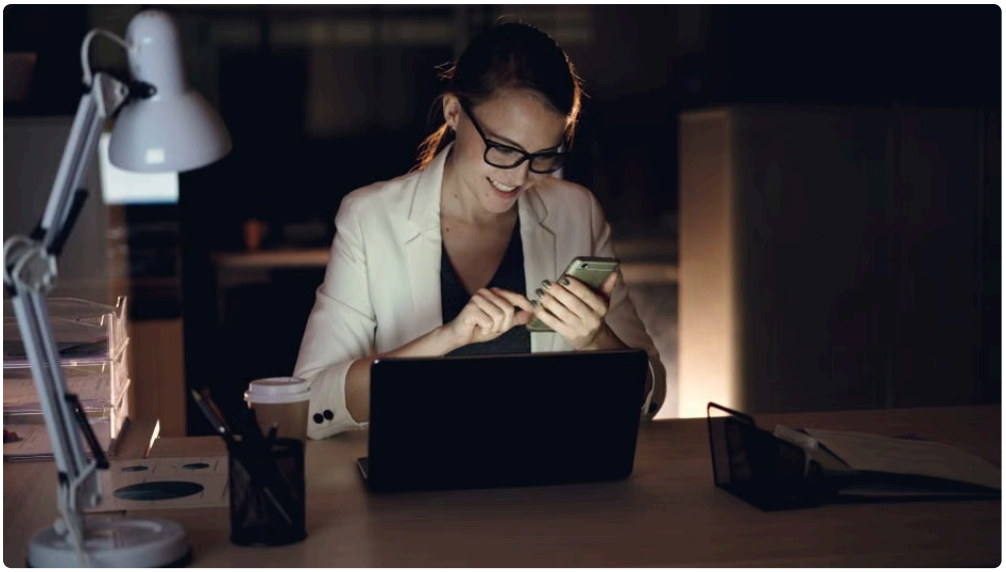
A workaround often starts with a practical problem: you cannot access a roster, a document will not open on your phone, or a team needs to share information quickly. But using an unapproved app, personal account, or device feature for patient or organizational data can create privacy and security risks—and may conflict with your employer's policies.



The goal is not to blame anyone for trying to keep work moving. It is to describe the problem clearly, explain the risk, and **raise it through a workplace channel** so the organization can consider a **supported tool request** or another **policy-aligned fix**.

This guide is for UK healthcare and other regulated workplace settings. It draws on the Information Commissioner's Office (ICO) guidance, including its material on working securely and working from home securely. Your employer's policies and instructions take priority for your specific systems and situation.

## Start with the employer's device and BYOD policy

Before asking for a new app or access route, check your employer's current policy on devices and "bring your own device" (BYOD). BYOD usually means using a personally owned phone, tablet, or computer for work. The policy should explain whether this is allowed, what work activities are permitted, and what controls are required.

Look for the relevant documents on your staff intranet or ask your manager, IT service desk, information governance team, or data protection officer (DPO) where to find them. Search terms may include "mobile devices," "remote access," "acceptable use," "information security," "BYOD," and "working from home."

Check for practical details, such as whether the organization requires a managed app, device registration, multi-factor authentication, encryption, automatic locking, or the ability to remove work data from a device. Also check whether personal devices are prohibited for particular tasks, even if a work app is available.

Do not assume that a folder, separate home screen, or different user profile makes a personal device safe for work data. Separation can help with organization, but it is not a substitute for approval, appropriate security controls, and a clear policy.

Question to check Why it matters Is this device approved for work use? Policy may restrict access to certain devices or data. Which apps and storage locations are authorized? An app that is convenient may not be approved for patient or organizational data. What happens if the device is lost or access needs to be removed? Staff need a

defined route for reporting, support, and protecting work information. Are there rules for notifications, screenshots, or downloads? These features can expose information outside the approved work system.

## Be clear about the problem, not just the app you want

A manager can act more easily when the request describes the work task and the barrier. “Can we get a secure app?” is difficult to assess. “The rota is available only through a system I cannot access from the ward device, so staff are copying shifts into a group chat” gives the manager a situation to investigate.

Describe what people are trying to do, how often the problem occurs, who is affected, and what impact it has on safe or timely work. Keep the explanation factual. Avoid including identifiable patient information in an email or ticket unless the approved process specifically requires it.

If a workaround is already in use, explain it without spreading the information further. Do not forward messages, export records, or attach patient details just to demonstrate the issue. Instead, describe the type of information involved and ask the information governance or security team how to provide any necessary evidence safely.

### Use a short, practical problem statement

- **Task:** What work needs to be done?
- **Barrier:** What prevents staff from using the approved route?
- **Workaround:** What are people currently doing, if anything?
- **Risk or impact:** What could go wrong, or what delay is occurring?
- **Request:** What decision, advice, or supported option do you need?

## Keep patient and organizational data in approved systems

For patient and organizational data, use only systems approved by your employer for that type of information. That may mean a specific clinical record, document platform, secure messaging service, or remote-access method. An app being available in a public app store—or already installed on a device—does not make it approved for work.

Do not move work information to a personal email account, consumer file-sharing service, private messaging app, or unapproved note-taking tool to get around an access problem. Do not use screenshots or camera photos as a substitute for an approved record. Those steps can create extra copies that are harder to control, retain, or remove.

The ICO’s UK GDPR guidance explains the importance of protecting personal information and applying appropriate security. Its guidance on working securely and working from home securely is useful when considering access, devices, communications, and the environment in which work is done. It does not approve a particular product for your employer. Your organization must decide which systems staff may use and how they should be configured.

If an approved system is too slow, unavailable, or difficult to use, say so. Last month, I was working with a client who thought they could save money but ended up paying more.. A request for a supported tool should include the actual workflow issue—for example, access from a particular work location, compatibility with an existing system, or a need for a documented handover route. This gives IT and information governance staff something concrete to assess.

## Separate entertainment from clinical work on a device

If your employer permits a personal device for work, keep work and entertainment distinct in the way the policy requires. Use the approved work app or managed work area, if one is provided. Do not copy work files into personal photo libraries, personal cloud backups, or entertainment apps. Do not share a device login with family members or colleagues.

Keep work accounts separate from personal accounts where your employer's setup allows it. That can reduce accidental mixing, but it does not turn an unapproved app or storage location into a safe place for work data. Follow the organization's instructions for downloading, saving, printing, or deleting work material.

Also consider what appears when you switch between apps. A notification banner, recent-apps preview, or shared screen can reveal information to someone nearby. Avoid opening work information where other people can see it, and follow local rules for using devices in clinical areas.

## Check lock-screen previews and notification privacy

Lock-screen previews are an easy-to-miss exposure. A phone may display message text, a patient name, a meeting title, or a work alert even while the device is locked. That can happen in a staff room, on public transport, or while the device is sitting on a desk.

If personal-device work use is permitted, check your employer's instructions for notifications. Where policy allows, set the lock screen to hide sensitive message content or show only that a notification has arrived. You may also be able to turn off previews for particular apps. Do not disable a required security or clinical alert without checking with the relevant team.

Then test the setting on the actual lock screen—not just in the settings menu. Lock the device and trigger a notification from the relevant work app, or use the organization's recommended test method. Check what a person standing nearby could read. If you cannot control the preview, or you are unsure what the policy requires, ask IT or information governance before using the device for work.

## Make a specific, workable request

Your manager may not be able to approve a new system alone. They may need advice from IT, information security, information governance, procurement, or the DPO. Frame the request as a route to a safe solution, rather than as a demand for one particular product.

A useful request can include the following:

- The task staff need to complete and the current approved route.
- The point at which that route fails or becomes impractical.
- The type of data involved, without including identifiable examples.
- How many staff or shifts are affected and how often the issue occurs.
- Any workaround that has emerged, described without sharing the data itself.
- The options you would like the organization to assess, such as improved access to an existing system, a managed device, or an approved alternative.
- Who should own the next step and when you can follow up.

Keep the request proportionate. You do not need to solve the technical or legal question yourself. Your role is to identify the operational need and ask the right workplace channel to assess it.

## Example wording for a conversation or message

You could adapt this wording for a one-to-one conversation, staff meeting, service desk ticket, or approved workplace reporting route:

“I’d like to raise a recurring access problem through the right workplace channel. Staff need to [describe task], but the approved system is difficult to use when [describe the barrier]. I’m aware that patient and organizational information should stay in approved systems. The current workaround appears to be [brief, factual description, without patient details], and I’m concerned it may not align with our device or information-handling policy. Could we ask IT and information governance to assess a supported option? I can provide examples of the workflow issue through an approved route. Who should own this request, and when would be a reasonable time to review it?”. Exactly.

This wording makes three things clear: the work need, the concern about the workaround, and the request for an organization-led decision. It also avoids implying that the manager should approve an app without the necessary checks.

## Use the right workplace channel and follow up

Start with your line manager unless your policy names another route. Depending on the issue, you may also need the IT service desk, information governance team, security team, DPO, or a formal risk-reporting process. Follow your organization’s instructions for logging concerns and include only information that the channel needs.

Ask for a clear next step: a ticket number, a named team, a policy reference, or a date for an update. If the answer is “we do not have a solution,” ask what staff should do instead. A safe alternative might be access to an existing approved workstation, a managed device, or a revised workflow. Do not treat silence or a colleague’s informal suggestion as approval.

If the issue affects several teams or shifts, a short summary Visit website of frequency and impact can help. Keep a record of when you raised the request and what guidance you received, using an approved workplace record or channel.

## If the workaround may already have exposed information

If patient or organizational data may have been sent to an unapproved service, left visible, or stored somewhere it should not be, do not try to investigate by making extra copies or forwarding the material. Follow your employer’s incident-reporting process promptly and tell the appropriate manager or security/information governance contact. Give them the facts they need, such as what type of information may be involved, the system or device used, and when it happened.

Do not delete or alter material unless the incident team instructs you to do so; it may need to understand what happened and take appropriate action. If a device is lost, stolen, or accessed by someone else, use the organization’s urgent reporting route rather than waiting for a routine meeting.



## A simple checklist before you raise the request

1. Find the current device, BYOD, and information-handling policies.
2. Confirm which systems are approved for the data and task.
3. Write down the barrier and its effect, without including patient identifiers.
4. Describe any workaround factually and do not extend its use to gather evidence.
5. Ask for a supported tool request or policy-aligned fix through the correct workplace channel.
6. Check the lock-screen and notification behavior on the actual device if work use is allowed.
7. Agree who will assess the request and how you will receive an update.

A good conversation is not about accusing colleagues or naming a favorite app. It is about making the work problem visible, keeping data in approved systems, and giving the organization a clear opportunity to provide a supported solution. That is more useful—and safer—than letting a temporary workaround quietly become the normal way of working.

## ICO resources

- ICO: UK GDPR guidance and resources on security
- ICO: Working from home securely

Check the ICO website for current guidance, and consult your employer's policies for instructions that apply to your systems, devices, and role.