You finish a shift, open a file on your phone, and tap the cloud icon. A moment later, you realize it may have gone to your personal account instead of your employer's approved storage. It is an easy mistake to make when work and personal apps sit side by side—and a serious one if the file contains patient or organizational information.

The safest fix is not simply to slow down or "be careful." Build a repeatable check into the way you use your device: follow your employer's device policy, use approved storage, separate work from personal activity, and verify the destination before sharing or uploading. These steps help whether you work from home, travel between sites, or use a personal device under a bring-your-own-device (BYOD) arrangement.

## Start With Your Employer's Device Policy

Before changing settings or adding a work account, check your organization's BYOD and information-handling policies. They should explain whether personal devices can be used for work, which apps and storage services are approved, and what to do if a device is lost or information is sent to the wrong place.

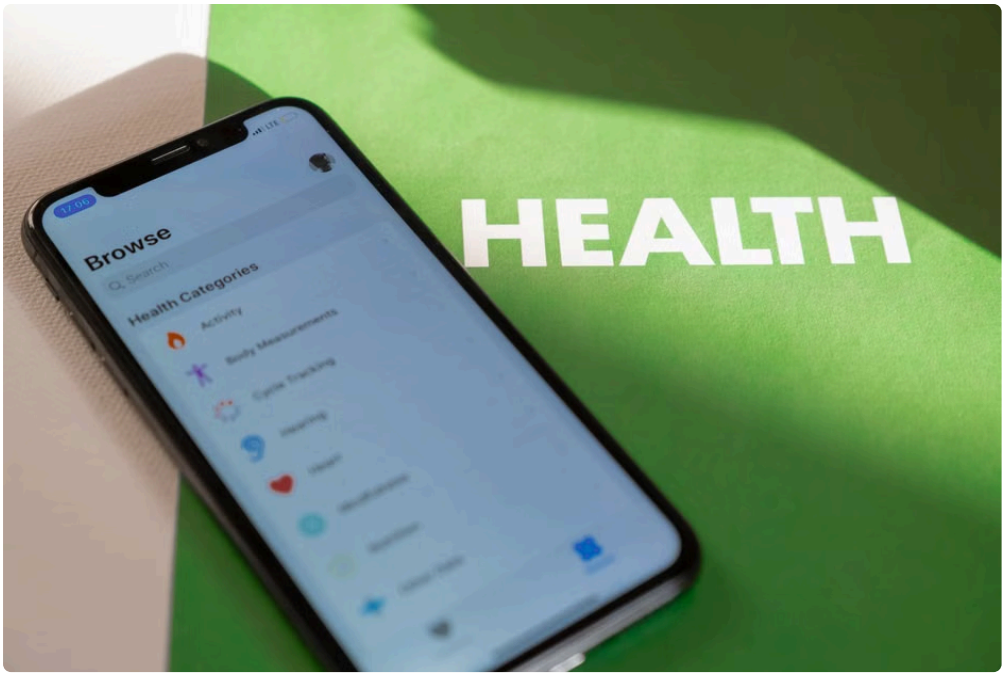
Do not assume that a service is approved just because it is well known, already installed, or included with your personal phone plan. Your employer may require a managed app, a work profile, a virtual desktop, or access through a particular portal. It may also prohibit downloading patient or organizational files to a personal device altogether.

If the policy is unclear, ask your manager, information governance team, IT service desk, or data protection officer before moving files. Do not use a personal email account as a workaround. If you cannot access an approved system, ask for the supported route.

### Check These Points Before You Begin

- Is this device allowed for the type of work you need to do?
- Which apps and cloud services are approved for patient and organizational data?
- Does the device need a work profile, management software, or additional security settings?
- Can files be downloaded locally, or must they stay in the approved system?
- Who should you contact if a file is uploaded or shared incorrectly?

Follow your organization's instructions even if they are less convenient than using a personal app. A separate folder or a clearly named album does not, by itself, make information secure.




## Use Approved Storage for Work Information

Keep patient and organizational data in the storage system your employer has approved for that purpose. Approved storage is more than a familiar brand name: the organization may have configured access controls, retention rules, auditing, and support around a specific account or service.

Do not treat all cloud accounts from the same provider as interchangeable. A work account and a personal account can look almost identical, use the same logo, and appear in the same share sheet. They may still have different owners, permissions, and security arrangements.

When choosing a storage location, use the route provided for the task—for example, the relevant work app or organization-managed file area. Avoid copying work files into personal cloud backups, personal photo libraries, consumer note apps, or other services that your employer has not approved.

### Make the Destination Obvious

Where your organization's setup allows it, give work and personal accounts distinct names or visual cues. For example, a work account may display your organization's name, while a personal account displays a private email address. Use a work-specific app or profile if your employer provides one.

These cues are reminders, not security controls. They can help you spot an error, but they do not turn an unapproved destination into an approved one. Keep the organization's rules as your deciding factor.

## Build a Reliable Upload Destination Check

A destination check is a short pause before you tap "Upload," "Save," or "Share." It is particularly useful when you have multiple cloud accounts signed in on one device. Make it a routine rather than a test of memory.

1. **Identify the file.** Confirm what you are handling and whether it contains patient, staff, or other organizational information.
2. **Open the approved work route.** Start from the employer's designated app, work profile, or portal instead of relying on a general device menu.

3. **Read the account name.** Check the account shown in the app or upload window. Look for your organization's account details, not just the provider's logo.
4. **Check the destination folder or site.** Confirm that the location is the intended work area and that it is appropriate for this file.
5. **Check the action.** Make sure you are uploading or saving to the expected place, rather than creating a public link or sharing with an unintended person.
6. **Verify the result.** If the file is important, check that it appears in the correct approved location before closing the app.

Do this check whenever you switch accounts, use a different app, respond to a share prompt, or upload after a software update. Do not rely on where the last file went; apps can remember different accounts for different tasks.

NHS approved cloud storage Moment What to check Before selecting a file Are you in the approved work app or work profile? At the upload screen Does the account name clearly identify your organization? Before confirming Is the destination the correct work folder, site, or record? After uploading Can you see the file in the intended approved location?

## Separate Entertainment From Clinical Work

Personal streaming, shopping, gaming, and social apps can make it harder to spot which account or app is active. Separation reduces wrong taps and makes work information easier to keep within the approved environment.

If your employer supports it, use a managed work profile or a separate work device. Follow the setup instructions rather than trying to create your own workaround. Keep work files inside work apps, and avoid opening them through personal apps that may automatically sync, back up, or offer a personal cloud account as the default.

On a shared or personal device, use clear boundaries:

- Open work files from the organization's approved app, not from a personal file manager unless policy allows it.
- Do not enable automatic backup of work files to a personal cloud account.
- Do not save work attachments into personal photo, notes, or downloads apps unless your employer explicitly permits it.
- When finishing work, sign out or switch profiles as directed by your organization.
- Keep work and personal account names visibly distinct where settings allow.

Separation is useful, but it is not a substitute for approved storage or device controls. A "Work" folder inside a personal cloud drive is still part of that personal cloud account.

## Protect Lock Screen Previews and Notifications

Even if a file stays in the correct cloud account, notifications can reveal information on a locked screen. Message previews, email subject lines, file names, and shared-document alerts may be visible to someone nearby or to a person who picks up the device.

Review notification privacy for work-related apps. Depending on your device and employer's instructions, you may be able to hide preview text, show notifications only after unlocking, or disable lock-screen notifications for selected apps. Avoid putting patient names or other sensitive details in notification text where you can choose a less revealing label.

Do not assume a setting worked because you changed a menu option. Test it on an actual lock screen. Lock the device and trigger a work notification, or ask a colleague to send a harmless test message. Check what appears before unlocking. If the preview still displays content, revisit the app's notification settings and the device's lock-screen privacy settings. Follow your organization's required configuration if it differs from general advice.

## Use the ICO's Guidance as a Practical Check

The UK Information Commissioner's Office (ICO) publishes guidance for organizations on working securely and working from home securely. Its practical themes include protecting devices, controlling access to information, and taking care when work is done outside the usual workplace.

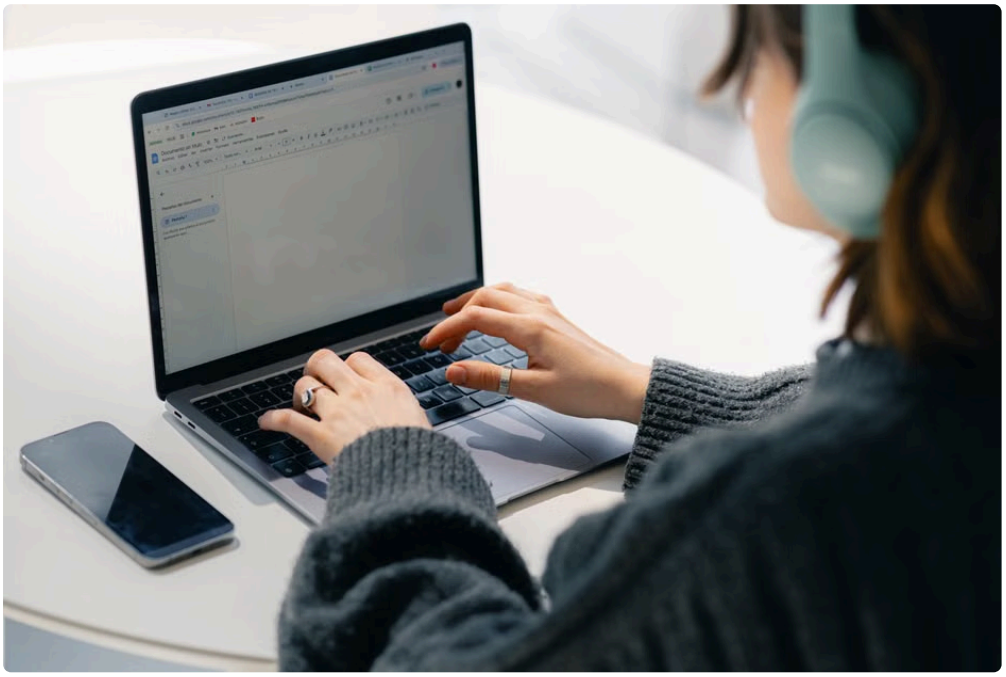
Use the ICO's working securely guidance and working from home securely guidance alongside your employer's policies. The guidance can help you understand the security principles, but it does not tell you which cloud service your particular organization has approved. Your local policy and IT instructions determine the permitted route for your work.

## If You Upload to the Wrong Account

If you think a work file may have gone to a personal or otherwise unapproved account, act promptly. Do not quietly delete it and assume the issue is resolved. Deletion may not remove copies from backups, synced devices, or shared locations, and your organization needs to assess what happened.

1. **Stop further sharing or syncing.** Do not forward the file or create additional copies.
2. **Record the facts.** Note what file was involved, when it was uploaded, which account or location was used, and whether anyone else could access it.
3. **Contact your organization promptly.** Use the incident-reporting route in your policy, such as your manager, IT service desk, information governance team, or data protection officer.
4. **Follow instructions.** Your organization may ask you to remove access, preserve information for review, or take other steps. Do not decide on your own that deleting the file is enough.

Report near misses, too. If you noticed the wrong account before confirming the upload, telling your team can help identify confusing app prompts or improve local instructions.



## A Short Routine to Remember

Before every work upload, ask: **Is this an approved device and app? Is this the right work account? Is this the right destination? Is the file staying within approved storage?** Then check notifications and lock-screen previews so work information is not exposed when the device is idle.

When multiple cloud accounts live on one device, the safest workflow is the one that makes the approved route clear and gives you a chance to catch a wrong tap. Start with your employer's BYOD policy, keep clinical and personal activity separate, verify the destination every time, and report mistakes promptly.