

Before the next access request

A decision guide for construction IT teams, project owners and their providers.

A company phone, a personal device and a client-issued login are different parts of the arrangement. Start with the work and the account owner before choosing the equipment.

Approach	When to consider it	Settle before approval
Company-managed phone	Daily work apps and a consistent supported setup.	Required apps, management, SIM, replacements, support and access permissions.
Controlled personal-device access	Tasks fit supported protected apps and an agreed work/personal boundary.	Platform, user type, licences, privacy, data movement and supported removal.
Restricted or temporary access	A defined task needs a narrower information set or app role.	Viewing/editing, downloads, offline use, account owner and review/end date.

Three questions to answer together

- What must this person actually do: view, edit, photograph, download or work offline?
- Who owns each account and system: your business, their employer, a client or another provider?
- Who approves the setup, supports it and confirms the change when the work ends?

One request. One agreed brief.

Fill in for one role or package of work. Save a copy for the project owner and IT.

Project / role / duration

Applications and the tasks to complete

Device owner and proposed arrangement

Account and system owners

Controls and privacy limits to confirm

Costs, support and replacement owner

Approval, review date and end-of-access owner

Ask the provider for a working arrangement

Use these checks to turn the decision sheet into an implementation brief.

Microsoft and identity

Confirm the account type, applications and licences. Microsoft lists the “Require app protection policy” Conditional Access grant as unsupported for B2B collaboration/direct connect users. Ask which supported controls cover your external-user arrangement.

Devices, SIMs and support

Confirm provisioning, replacement, helpdesk ownership, costs and any project allocation. A personal handset still needs a supported way to work.

Information and privacy

Agree permitted downloads, sharing and offline work. Explain what the organisation manages on a personal device. Test the required tasks before rolling out the policy.

Change and offboarding

Name the person who receives project changes. Separate permissions, app data, sessions and asset recovery; keep externally controlled actions open until confirmed.

Selective wipe applies to organisational data in supported protected apps and depends on the action completing. It does not remove every separately retained copy. Access revocation also depends on the application and session.

Sources and the next step

[Microsoft app protection overview](#)

[Microsoft external-user access controls](#)

[Microsoft selective wipe](#)

Use the guide to identify a decision or evidence gap. For a specific question, [contact Assured Digital](#). For a broader self-review, [explore the mobile-access diagnostic](#).