

A lot of intranet and portal projects aim to deliver functionality related to personalisation or customisation.

This may involve tailoring information based on staff role, delivering news relevant for specific offices, or limiting access to information based on seniority.

Any of these capabilities requires the system to know *who staff are*, the business unit they belong to, and where they sit in the real world.

Unfortunately, too many of these projects run aground before they start because a key piece of IT infrastructure has not been correctly put in place.

LDAP and Active Directory

Sitting invisibly behind the scenes in organisations is the ‘authentication’ platform run by IT. In simple terms, this contains the usernames and passwords staff use when they log on to their PCs each morning.

Over time, these details have been migrated into one of two standards: LDAP (an open industry standard) or Active Directory (the Microsoft variant of the same thing).

These expanded ‘directory services’ have the ability to store much more than just names and passwords. If configured to do so, they can contain all the information that is in the internal phone directory or staff directory, including job titles, business unit names, locations and more.

The most obvious benefit to come from putting in place these new standards is the progressive move towards ‘single sign-on’, allowing one username and password to be used across a wide range of corporate systems.

Crucially for intranet and portal projects, LDAP or Active Directory is also the source of the information needed to drive personalisation and customisation.

Instead of the intranet building its own database of staff information, staff details are drawn out of this directory service platform.

And this is where the problems become apparent, because these platforms are often not configured in a way that works for intranet projects.

Technology narrowly implemented

LDAP and Active Directory were originally deployed by IT to manage just usernames and passwords, as replacements for legacy platforms. The focus of these projects was on managing the technology transition, not adding extra functionality.

While usage has been somewhat expanded since, improvements to directory services have been driven solely by IT considerations. There has been little opportunity for business or information management areas to get involved in defining platform needs.

This means that even when details such as business unit are implemented, they are often captured in ways that don’t match how they are used in the business.

Capturing the right details

Fundamentally, LDAP or Active Directory needs to contain at least the following information to support personalisation and customisation:

- job title
- job role
- business unit
- office location
- direct manager

These details also need to be kept up to date, through direct integration with HR systems, as well as via self-service updates in the staff directory.

Start by talking with IT

While very technical, and far from sexy, underlying directory services are vital for the next generation of intranet and portal projects.

The starting point for intranet and portal teams must be to engage in discussions with IT about these platforms, to gain a clear understanding of what is in place, and how it works.

The necessary improvements to these underlying platforms must start well in advance of the intranet or portal work, and managed as a joint IT/business project. Only then will true personalisation become possible.