# Breaking Down Barriers Between Legal Firms and LawTech Adoption

One-Pager Selection

# Identity & Access Management (IAM)

Identity and access management refers to the framework put in place which provides the individuals in an organisation appropriate access to resources.

**Identity Experts**

## JML

Keep up with joiners, leavers and movers within the organisation, changing and revoking access automatically to safeguard sensitive information.
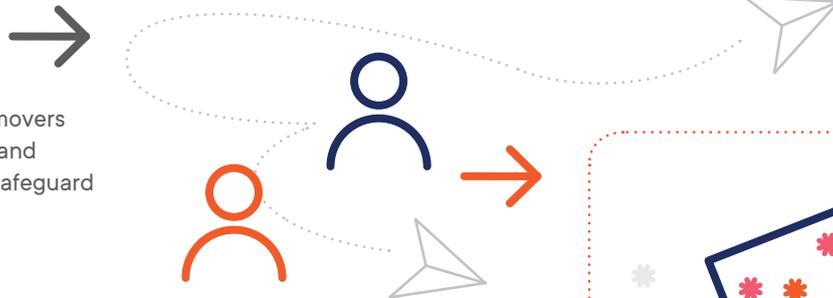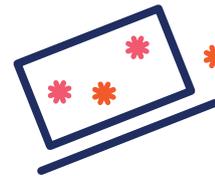
### Self-Service

✓ Gift users with the autonomy to manage their passwords and request access to sensitive information.

✓ Save on support costs by freeing your IT department from trivial tasks.

### Single sign-on

The days of passwords scribbled on post-it notes are over: with single sign-on (SSO), users can use one identity to manage different access permissions.

### Reporting

Understand who has access to data, and who has accessed it in the past, for a top-down view of the organisation's security.

### Facts

**42%**

A survey into IT managers' confidence around protecting their organisations showed that 42% of respondents admitted their uncertainty to prevent breaches caused by accidental or purposeful staff actions.

### Fresh start

**15**

Prevent duplicating pre-existing identities and unwittingly giving new starters years of amassed permissions.

**Newham London**

"We've got 15,000 students live at any one time, so to manually manage on-boarding and de-provisioning is a very onerous task for the IT team. Now, we have the automated management of staff and student account provisioning."
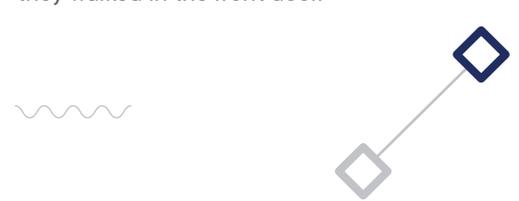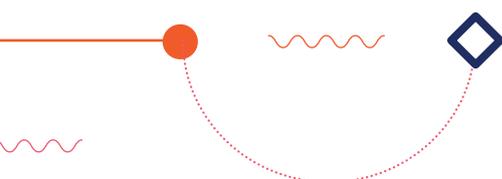
**Steve Parry,
Newham College**

## How Can IAM Help You?

Before IAM was implemented, a new employee would have to wait for up to one day for their system accesses to be manually provisioned, causing frustration and wasting productive time.

With IAM, accounts, permissions and passwords were ready for them when they walked in the front door.

# B2B Collaboration

Open yourself up to smart, secure collaboration by controlling access and safely sharing resources with external partners.

**Identity Experts**

## Reporting

Finite control over who has access to sensitive information.

## Limits Data Sharing

Prevent high-risk alternatives to sharing information, such as USBs and CD-ROMs.

## Share Internal Resources Safely

Be confident that only individuals with the right permissions can access internal resources.

## Did You Know?

Franchises can maintain consistency, reduce costs and ensure consolidation by separating franchisee usage, while still allowing them to use the same ticketing or support system as the franchisor.

## Keep Credentials

Previously, providing access for partners to internal or cloud based information required setting up VPNs, new accounts with yet another password. With B2B the external party can securely login using their own credentials with no additional software.
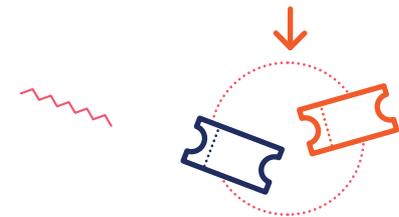
## Keep it Simple

Partners use their own credentials to gain access - meaning no need for complex configuration or duplicate users.

## Stay GDPR Compliant

Your collaborators can rest easy knowing their data is in safe hands.

## Empowering your collaborators

Organisations can invite B2B users to create an authenticated guest account, granting permission to access apps securely.

B2B User → Your Organisation → Cloud Apps → SaaS

On-Premises