Navigating the Expanded Right to Work Rules: What Shift Operators and HR Must Do

Published: September 15, 2026

Category: Workforce Security & Floor Verification

Reading Time: 4 minutes

In modern shift-based operations—from fulfillment warehouses and event halls to care homes and facilities management—digital onboarding has transformed how businesses verify new workers. Biometric IDVT and online Share Code checks have made remote verification fast and paperless.

However, digital verification on its own leaves a major operational loophole open: it verifies the document during registration, but it does not verify who actually shows up at the gate on Monday morning.

In high-turnover shift environments, "substitute working" and identity swapping are growing liabilities. If an unverified worker steps onto your shift floor using someone else's credentials, your digital onboarding check offers zero protection against Home Office civil penalties of up to £60,000 per worker.

To close this gap, forward-thinking operators are adopting the 2-Gate Defense model.

The Flaw in Single-Gate Onboarding

Traditional onboarding operates as a single gate:

- **Gate 1 (Remote Check):** The worker submits their passport or Share Code online. A Statutory Excuse profile is generated.

Once cleared, the worker is added to the shift roster. But what happens on the shift floor?

- In fast-paced sites, floor managers rarely re-verify physical identity at the gate.
- Bad actors take advantage of this gap by passing cleared account details to unregistered friends, family members, or illegal workers.
- During an unannounced Home Office or labour audit, discovering an unverified individual on site immediately destroys your legal defense—regardless of how compliant your

digital onboarding software was.

Introducing the "2-Gate Defense" Model

To achieve complete compliance, identity verification must bridge the gap between the digital registration desk and the physical shift floor. The **2-Gate Defense** creates an airtight, two-step verification shield:

Gate 1: Certified Remote Onboarding

Before setting foot on site, the worker completes an online check:

- **UK/Irish Nationals:** Verified via government-certified biometric IDVT (liveness and document checks).
- **Non-UK Nationals:** Verified via official Home Office Share Code validation.

Gate 2: On-Site Digital Wallet Verification

Once cleared at Gate 1, the worker receives a tamper-proof Digital Wallet Pass directly in their Apple Wallet or Google Wallet, featuring their verified photo and cleared status.

When arriving for a shift:

1. The floor manager or shift lead opens their standard smartphone camera or management tool.
2. The manager scans the worker's Digital Wallet Pass QR code at the gate.
3. The system instantly confirms match and authorization in 1 second—verifying that the person standing on the floor is the exact individual cleared at Gate 1.

Why Floor Scans Are Essential for Shift Operators

1. **Stops Identity Swapping Instantly:** Unregistered substitutes cannot produce a valid, cryptographically signed wallet pass with matching photo identification.
2. **Zero Overhead for Managers:** Shift leads do not need to inspect physical passports or handle paper files on a busy warehouse floor.
3. **Immutable Audit Trails:** Every Gate 2 scan generates a time-stamped log, proving to Home Office inspectors that physical identity was verified at the exact moment work commenced.

The Bottom Line

A digital check that stops at the onboarding desk is only half a compliance strategy. Combining digital IDVT at Gate 1 with rapid QR verification at Gate 2 gives shift operators complete, end-to-end protection against illegal working fines and site impersonation.

About DashCrew®

DashCrew® provides zero-subscription, Pay-As-You-Go Right to Work software for shift-based businesses and charities. Protect your organization against £60k civil penalties with our quick 2-Gate biometric and QR compliance shield.