



Personnel Security Policy

This policy sets out how Novi (Forward Ladies Limited) ensures the people who work with us — employees, associates, and contractors — are appropriately vetted and onboarded, and that expectations of conduct are clear throughout their time working with us, proportionate to the size of the business.

1. Roles and Responsibility

Personnel-related decisions rest with the director. Day-to-day onboarding administration — right to work checks, references, contracts, and the staff manual — is managed by our outsourced HR provider.

2. Pre-Employment Checks

- Right to work in the UK is verified for all new employees before they start.
- Satisfactory written references are obtained from an employee's former employer for the 3 years immediately preceding their engagement, where that role involves responsibility for money, accounts, or goods — consistent with the terms of our Professional Indemnity insurance.
- Associates and contractors who process personal data on our behalf are engaged under our Associate Data Processing Agreement and are expected to comply with our Code of Conduct.
- For any role involving a work experience placement, internship, or other engagement with under-18s, enhanced DBS checks and consent arrangements apply, as set out in our Safeguarding Policy.

3. Onboarding

Every new employee is introduced, through our outsourced HR provider, to:

- Our employment contract and staff manual, covering conditions of service and exit terms
- Our Code of Conduct
- Our Confidentiality Policy
- Our Cyber Security & Data Protection Policy, including our expectations of security-conscious behaviour (Section 2)

Associates and contractors are introduced to the relevant policies for their engagement — typically our Code of Conduct, Confidentiality Policy, and Associate Data Processing Agreement — before beginning work.

4. Ongoing Personnel Security

Our policies are reinforced on an ongoing basis, not communicated once, through our Organisational Learning and Continuous Improvement process (Section 8 of our Cyber Security & Data Protection Policy). Any change to a policy relevant to personnel security is communicated directly to employees and associates.

5. Leavers

When an employee or associate's engagement with us ends:

- Access to business systems, email, and cloud accounts is revoked
- Any company devices or physical materials are returned

- Where the leaver processed personal data on our behalf, data is deleted or returned in line with our Cyber Security & Data Protection Policy and, where applicable, our Associate Data Processing Agreement

6. National Security Vetting

Novi does not currently undertake formal National Security Vetting (e.g. BPSS or SC-level checks) as standard practice, given the nature of our work. Where a client's contract requires a specific vetting level for our scope of work, we would welcome confirmation of that requirement so we can consider how to meet it.

7. Review

This policy is reviewed at least annually by Griselda Togobo.