



---

# Remote Working Policy

Pronounced80 Solutions Limited

*Freeing business from the tyranny of legacy software*

Version 1.0 | Effective: May 2026 | Review: Annual



## 1. Purpose

To set out requirements for secure and effective remote working.

## 2. Scope

All personnel working from any location other than a client site.

## 3. Working Environment

- Suitable, private workspace with secure storage for any physical materials.
- Screens not visible to unauthorised persons.
- Confidential calls held in private settings.

## 4. Connectivity

- Use of trusted networks; avoid untrusted public Wi-Fi for client work, or use VPN where required.
- Home routers configured with strong admin credentials and current firmware.

## 5. Devices

- Devices comply with the Mobile Device Policy and BYOD Policy.
- Full-disk encryption, screen lock, automatic updates and endpoint protection enabled.

## 6. Data Handling

- Client data accessed only via approved systems.
- No printing of client confidential data unless required and authorised; secure disposal if printed.
- No storage of client confidential data on personal accounts or unmanaged cloud services.

## 7. Access and Authentication

- MFA enforced where supported.
- Access aligned with the Access Control Policy.

## 8. Incidents

- Lost/stolen devices, suspected compromise or unauthorised access reported immediately to the Director.

## 9. Wellbeing

- Reasonable working hours, breaks and ergonomic setup encouraged.