GDPR – Working from Home Policy

Purpose

This Policy outlines how Quest Training ensures compliance with the General Data Protection Regulation (GDPR) when employees work from home, or remotely. It aims to protect personal data from unauthorised access, loss, or disclosure.

Overview

This Policy applies to:

- All personal data processed by the organisation during remote work
- Employees, contractors, and other personnel who have access to personal data
- Company-owned and personal devices used for work purposes

All remote work activities involving personal data must follow GDPR principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Expectations & Responsibilities

Employees:

- Must remain reachable via company communication tools (e.g. - Teams, Email, work mobile)
- Are expected to maintain, or exceed, on-site performance levels
- Must join scheduled, virtual meetings, and respond to messages promptly
- Must keep their calendar updated and share their work status with their team

Device Security

- All devices used for work must be password-protected and encrypted
- Only company-approved software and devices may be used to process personal data
- Antivirus and security software must be installed and up-to-date
- Employees must use secure, password-protected Wi-Fi networks
- Use of VPN is mandatory when accessing company systems remotely

Data Storage

- No personal data should be stored on personal devices or local drives
- Only use company cloud services (e.g., OneDrive, SharePoint, Microsoft Teams) to store documents
- Use only approved communication tools (e.g., Microsoft Teams, company email, Whatsapp)
- Avoid discussing personal data over unencrypted messaging apps
- Remote workers should only access personal data necessary for their role
- Shared, or family, use of work devices is strictly prohibited

Incident Reporting

- Any suspected data breach must be reported to the Data Protection Officer (DPO) immediately
- Reports should include details, such as: what data may have been affected and how the breach occurred

Equipment & Support

Company Provided:

- Laptop or desktop computer
- Necessary software and licenses
- VPN access
- IT support during business hours
- Work mobile phone

Training

All staff must complete GDPR and data protection training annually.

- Employees must confirm they have read and understood this Policy before remote access is granted
- Breaches of this Policy may result in disciplinary action, up to and including termination of contract
- Legal action may be taken, where appropriate

Termination or Suspension of working from home arrangements

Quest training reserves the right to suspend, or terminate, any working from home arrangements based on:

- Poor performance
- Security or Policy violations
- Changes in role responsibilities

The organisation will periodically review remote working practices to ensure compliance.

Audits will be conducted to ensure adherence to this Policy.

This Policy will be reviewed, yearly, as part of Quest Training's quality assurance cycle and GDPR compliance and commitment.

I confirm that this Policy is authorised and approved by Abbie Fulks – Managing Director.

Signature:  Date: 25/7/2025

Implementation date: 25/07/2025

Next review date: July 2026