**Remote Working Policy**

**Introduction**

Remote working is a working style that allows someone to work outside of a traditional office environment. This policy is intended to outline guidelines for employees who work from a location other than our offices.

**Policy Scope:**

The policy applies to employees who, by prior agreement with their line manager, work part or all of their week from a location other than [COMPANY NAME] offices. Remote agreements may be permanent or temporary as per agreement, however [COMPANY NAME] Reserves the right to amend any remote working agreement in line with business requirements

[COMPANY NAME] reserves the right to deny any remote working request in line with business requirements.

**Remote Working Conditions:**

To ensure that employee welfare and performance will not suffer in remote work arrangements, we advise our remote employees to:

* Choose a quiet and distraction-free working space.
* Have an internet connection that’s adequate for their job.
* Dedicate their full attention to their job duties during working hours.
* Adhere to break and attendance schedules agreed upon with their manager and in line with the Organisation of Working Time Act 1997.
* Ensure their schedules overlap with those of their team members where possible.
* Ensure that their workspace is set up in line with [COMPANY NAME]’s health and safety statement
* [COMPANY NAME] reserves the right to inspect any remote work location in order to ensure compliance with the safety and health at work act 2005.

**Data Protection:**

While working remotely all employees must ensure that they remain compliant with General Data Protection Regulations (GDPR). [COMPANY NAME] requires employees working remotely to ensure the following:

* No work is to be saved to the hard-drive of any device, secure remote access has been provided to save work to shared drives.
* No work is to be done on any personal device while any other application (e.g. social media, games, websites, banking) is open.
* Work must not be left unattended or on ‘stand-by.’ If taking a break, save and close work.
* Do not use your password for any personal applications or media.
* All devices used for work must be password protected, and locked or turned off when not in use.
* Do not work with confidential information while on unsecured or public Wi-Fi.
* Ensure that any printed confidential information is securely stored or correctly and confidentially disposed of.
* Do not leave any confidential information in printed or electronic form unattended at any time. If you have printed information please ensure your workspace has lockable storage and only you have access.

Please refer to [COMPANY NAME]’s data protection policy for further guidance on correct procedure when dealing with confidential information.

**Compliance with Policies**

Our remote employees must follow our company’s policies like their office-based colleagues. Examples of policies that all employees should abide by are:

* Attendance
* Social Media
* Confidentiality
* Data Protection
* Employee Code of Conduct
* Bullying & Harassment
* Dress Code
* Compensation and Benefits
* Data Protection

This list is not exhaustive, and all policies and procedures in place must continue to be observed while working remotely. Annual salary and any other benefits are determined by job role. Any prior agreements are not altered by a remote working agreement.

### **Equipment**

[COMPANY NAME] will provide our remote employees with equipment that is essential to their job duties, like laptops, headsets and cell phones (when applicable.) We will install VPN and company-required software when employees receive their equipment. We will not provide secondary equipment (e.g. printers and screens.)

Equipment that we provide is company property. Employees must keep it safe and avoid any misuse. Specifically, employees must:

* Keep their equipment password protected.
* Store equipment in a safe and clean space when not in use.
* Follow all data encryption, protection standards and settings.
* Refrain from downloading suspicious, unauthorized or illegal software.

**Policy Review:**

This policy will be reviewed on an annual basis.