Hybrid Working Policy

Introduction

The Company is committed to reducing our impact on the environment, provides a supportive and productive work environment that attracts and retains employees and promotes a positive work/life balance. This policy aims to describe our approach to hybrid working and the working arrangements that will apply in relation to you altering your time between the traditional working environment of the workplace and working from a remote location (typically your home). This policy further describes the working arrangements that will apply to Company employees and workers working from home or considering working from home at any time.

Entitlement

Company supports hybrid / remote working for only certain roles and reasons. Hybrid working is a cooperative arrangement, based on the needs of the Company, each employee's department, and role, that allows employees to work at alternate work locations for all or part of their work week.

Although some positions may require remote work, it is typically a work arrangement determined by employees' supervisors and line managers in which eligible employees fulfil their job responsibilities at a site other than their onsite work location (typically your home) during regularly scheduled work hours.

Hybrid arrangement

Expected attendance

The Company has an expectation that you will spend 1 day per week at the workplace. Your line manager will agree which days you are expected to work at the workplace and the days on which you are expected to work from home/remotely.

The Company understands that on occasion there may be a need for further flexibility in relation to hybrid working, depending on individual circumstances.

Should you require a hybrid approach which differs from this policy, please speak to your line manager. Your line manager's agreement will be required to depart from the aforementioned arrangement.

Flexibility

The Company reserves the right to vary or terminate the hybrid working arrangement at any time, due to a change in business needs, performance concerns, or if there is a change to your role.

As a hybrid worker, it is essential that you remain completely flexible to meet the needs of the Company. You may be required to vary your particular days or times in the workplace on occasion, for business reasons, including any requirement for you to attend training or meetings. On such occasions, you will be given as much notice as possible.

You may be required to work from home/remotely, when you would otherwise be expected to attend the workplace, for operational needs, or for pandemic-related reasons, for example in circumstances of lockdown/government guidance that staff should work from home where possible. In these instances, you will be given as much notice as possible.

Attending the workplace

You are required, on request, to attend the workplace for purposes such as training, performance assessment and team briefings. The dates and times of such visits will normally be agreed with you in advance.
You will be provided with your own permanent workstation, or practice hot desking (depends on the role). At the end of each day, you must ensure that you leave the hot desk clean and tidy and ensure that your equipment is either taken with you or secured away in your desk drawers/cupboard. The company takes no responsibility for any personal items left behind.

Contact

Whilst you work from home/remotely, the Company will normally expect you to maintain regular contact with your line manager.

Health and safety

Home/remote location

The Company is obliged under health and safety legislation to ensure the health and safety of all workers. The Company is therefore required to ensure that:

- all equipment and systems of work in your home/remote location are safe;
- all articles and substances are handled and stored safely;
- an assessment of your workstation is conducted;
- staff contact Human Resources immediately of any concerns or injuries sustained whilst working from home;
- ensure no lose cabling is on the floor to avoid trips or falls or damage to the cables;
- do not overload the socket outlets;
- information and training on the safe use of equipment, including display screen equipment, is provided to you; and
- risk assessments and Display Screening Assessments are carried out in respect of the work you are carrying out at least annually or if your work station/location changes.

Employees are expected to maintain their home workspace in a safe manner, free from safety hazards.

If you work from home you have a duty to ensure, in so far as is reasonably practicable, that you work in a safe manner and that you follow all health and safety instructions issued by the Company from time to time.

As you may be working on your own whilst working remotely, you may be considered to be a 'lone worker', which means, you are expected to maintain a presence with your department/ colleagues to ensure your wellbeing. If, at any point whilst working remotely you do not feel or you have any health and safety or a wellbeing related problem, contact your line manager immediately.

Working time

Whether you are working in the workplace or your home/remote location, you must ensure that you take adequate rest breaks as required by the Working Time Regulations 1998. For workers aged 18 and over this includes:

- taking a break during each working day of at least 20 minutes, during which you must stop work;
- ensuring that you have a daily rest break of at least 11 continuous hours, i.e. the time period between stopping work one day and beginning work the next day must not be less than 11 hours; and
- having at least one complete day each week when no work is done.

Workplace/Office

The following measures for the workplace have been implemented:

- complying with all current Government's guidance

As a hybrid worker, it is essential that you follow the safety measures implemented by the Company or the Government. Any failure to comply with such measures may lead to disciplinary action in accordance with the Company's disciplinary procedure.

Insurance and legal considerations

You are responsible for checking that all home and contents insurance policies provide adequate cover for the fact that you work from home/remotely. You will remain covered by the Company's public and personal liability insurance policy for activities involved in the performance of your duties for as long as you comply with all Company policies and procedures. Should it be found there was breach of any of them, company insurance will not come to place an you may be liable for any damage, loss or any cost associated with the relevant situation.

Mortgage or rental agreements

As a hybrid worker you are solely responsible for checking applicable mortgage or rental agreements to ensure that you are permitted to work from home/remotely, and for obtaining any requisite permission to work from the home/remote location.

Additional expenses

The company will not reimburse any additional expenses associated with working from home. This includes but it is not limited to home office supplies, gas, electricity or internet, furniture or costs such as repairs.

Equipment whilst working from home/remotely

Interr does not provide hybrid employees with equipment or office furnishings for their home offices. Employees are solely responsible for the configuration of and all the expenses and services associated with remote workspace.

Employees are responsible for equipping and maintaining their home offices so that they can accomplish their work in an efficient and expeditious manner, ensuring health and safety and confidentiality whilst working from home.

However, all IT equipment, such as computers, laptops, screens or printers to allow you to work from home/remotely will be provided by the Company and maintained (and replaced when necessary) by the Company.

It is your duty to ensure that proper care is taken of the equipment and materials provided. You should also ensure that your broadband speed and mobile phone reception is of a standard which allows you to be able to perform your duties to an acceptable level.

If equipment relied upon as a condition for hybrid working is not operational, the employee will be required to either report to the office work location or make a request for time off under the appropriate Company policy.

On termination of your employment or contract for any reason, you must return all equipment and documents belonging to the Company.

Where the Company supplied a hybrid worker with software, hardware or other materials to perform the Company's business remotely, Interr assumes all risks of loss or damage to these items unless such loss or damage occurs due to the telecommuter's negligence. The Company expressly disclaims any responsibility for loss or damage to persons or property caused by, or arising out of the usage of any equipment provided to the hybrid worker, if not used in accordance with Company policies / procedures or by negligence of the user.

Information Security whilst working from home/remotely

The security of Interr's property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable and prudent precautions must be taken to protect Company's hardware, software, and information from theft, damage, and misuse.

The objective is to ensure the confidentiality, integrity, and availability of company information while employees work in various locations.

You must not allow members of your family or third parties who are not employed or engaged by the Company to access or use the Company's equipment, data or assets.

You are responsible for keeping all documents and information associated with the Company's business secure at all times.
Specifically, you are under a duty to:

- keep filing cabinets and drawers locked when they are not being used;
- ensure all confidential information is stored and disposed of in line with Company guidelines and not household waste disposal;
- delete or destroy any confidential information in any form in your possession when asked to do so by the Company or as soon when no longer used;

- not remove any sensitive information from the Company's premises without written management approval;
- leave Company equipment or information out of sight (e.g. laptops, mobile phones, documentation, etc);
- multi-factor authentication must be enabled for all remote access to company systems, providing an additional layer of security;
- secure your work area to prevent unauthorised access to the company assets, data or information;
- complete an annual information security checklist for their workstation to ensure compliance and adequacy of protection of information security
- keep all documentation belonging to the Company under lock and key at all times except when in use; and
- set up and use unique passwords for the computer and any other digital devices.

Approved Remote Worker Equipment
Employees working remotely must use company-provided computers and equipment unless other devices have been approved by the Information Security Manager/CEO.

The computer and any other equipment provided by the Company for you must be used only for work-related purposes and must not be used by any other member of your family or third party at any time or for any other purpose.

It is the Company's policy that all equipment, including computer equipment, and materials necessary for you to work from home will be provided by the Company and maintained (and replaced when necessary) by the Company. It is your duty to ensure that proper care is taken of equipment and materials provided by the Company.

On termination of your employment or contract for any reason, you are required to return all equipment, data, end point devices and documents. The Company will have the right to inspect your home at an agreed time to inspect all has been returned.

Personally Owned Information systems
Remote workers must not use their own mobile computing devices, computers, computer peripherals, or computer software for Company's related business without prior written authorisation from their supervisor/line manager and as approved by the Information Security Managers (IT System Administrators).

Malware Protection Software
All systems that access Interr's networks remotely must have an anti-malware/anti-virus. package approved by the Company and running.

Remote Access to Networks
All remote access to Interr's networks where required must be made through approved Remote Access points that are controlled by the IT System Administrators.

Screen Positioning
The display screens for all systems used to handle Interr's information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

Separate Room or Workspace
Whenever possible, remote working should be done in a separate room or workspace that can be secured from the rest of the house or coworking space and sensitive conversation cannot be overheard.

Inspections of Remote Working Environments
Interr maintains the right to conduct inspections of hybrid/ home working locations with one or more days advance notice.

Remote Working Environmental Controls
Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

Encryption and Boot Protection
All computers used for remote working (including mobile devices, laptops, tablets, and other transportable computers) which contain sensitive Company information must consistently employ both hard disk encryption for all data files and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the Information Technology Team.

Backup Procedures
Remote workers are responsible for ensuring that their remote systems and data are backed up automatically through the automated back-up system or in accordance with Company procedures.

Changes to Configurations and Software
On the Company's supplied computer hardware, workers must not change the operating system configuration or install new software. This is already disabled, but if such changes are required, they must be performed through the Information Technology Team with remote system maintenance software, with a prior approval from the Information Security Manager (IT System Administrators).

Changes to Hardware
Remote working computer equipment supplied by the Company must not be altered or added to in any way without prior knowledge and authorization from the Information Security Manager (IT System Administrators). This is currently disabled.

Paper Records Disposal
All printed copies of sensitive Company information must be crosscut shredded for disposal. Hybrid workers must not throw away Company's sensitive information in the wastebaskets or other publicly-accessible trash containers. Sensitive information must be retained in a lockable and secure cabinets until it can be shredded, or destroyed with other approved methods.

Shredders
Remote workers who are required to print any sensitive information should have an approved crosscut shredder to appropriately dispose of printed versions of sensitive information. If a shredder is not available at home, hybrid workers must securely take the sensitive information to the Interr's Head Office and shred in the designated shredders.

Rules and procedures
As a hybrid worker you are still subject to the Company's policies and rules. In the event of sickness or absence for any other reason you must comply with the absence reporting procedure. In the event of any meetings such as disciplinary or grievance you will normally be required to attend the Company's premises.

All employees working from home must ensure that they adhere to all Interr's policies, procedures and guidance especially in relation to but not limited Information Security, Information Security, Data Protection, Computer Policy, Clear Desk and Screen Policy, Mobile Phone and Health and Safety and treat current home working as though they are in the office.

Policy Review and Assessment
This policy may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024