# Work from Home and Working Remotely Policy

## Policy Objectives

In general, as a company we recognise that working from home is beneficial to our employees and the company in terms of work life balance, and sometimes it is necessary.

There are clear benefits to remote working for employees to gain better control of the elusive 'work life balance' and flexible working patterns, and from a company perspective the possibility of remote working may assist us to attract and retain staff with the benefit of lower costs and greater productivity.

This policy aims to provide the guidelines for making an application to work from home and the considerations which must be adhered to when working from home or working remotely occurs.

## Scope

This policy applies to all direct employees.

## Are employees allowed to work from home or work remotely?

An employee who wishes to request permission to work remotely must have exceeded their probationary period plus three months. This means that the maximum period of waiting time before an employee can apply to work remotely will be one year of service, this accommodates an extension of probationary period.

In principle, employees are allowed to work from home or work remotely only if their job duties permit it. People who are obliged to come in direct physical contact with customers, clients, stakeholders or in direct supervision of staff are not eligible to telecommute under this policy. Employees who carry out most of their work on a computer can occasionally work off-site.

The decision to permit remote working will be in accordance with the Remote Working Role Assessment Policy and Procedure.

## Place of Work

The place of work has changed to an address of the employees choosing. The employee is obligated to advise the company of the address where they are working from.

## Hours of work

The employee is obligated to abide by the requirements of the Organisation of Working Time Act in the carrying out of their duties remotely, this includes taking breaks, recording hours of work and submitting a time sheet that verifies both working hours and breaks.

## Policy elements

During normal time, Employees work from home or telecommute when they complete their work at a place located outside of our company's premises. They may work from home:

- Full-time
- On certain days
- Every day - dividing their schedule between being present at the office and working from a remote location.

Work from home arrangements can be occasional, temporary or permanent.

## Requesting Work from Home Procedure

During normal time where remote working is optional, when employees plan to work from home or work remotely, this procedure must be followed:

- Employees file a request in writing to their Manager/Supervisor/Human Resources Manager at least [two days] in advance.

- The Manager will consider the application giving due consideration to:

    - Is the employee eligible by nature of their job?
    - Are there any cybersecurity and data privacy concerns?
    - Will collaboration with the employee's team become difficult?
    - Do employees have the necessary equipment or software installed at home?
    - What are the conditions of employees' home or alternative place of work (noise, internet connection etc.)

- If the work from home arrangement spans for more than a week, managers and team members should meet to discuss details and set specific goals, schedules and deadlines.

- Employees who need to work from home for unforeseen reasons (e.g. illness or temporary difficult commute) should file their request as soon as possible, so managers can consider and approve it.

## Remote Working Arrangements – Best Practice

It is essential that the employee places themselves in a dedicated, distraction free area, in so far as possible. Somewhere quite would be preferable.

Ensure that the working arrangements include a comfortable chair, table, and access to an internet connection and phone.

Establish dedicated working times where the employee's full attention can be directed towards their duties and tasks. Where the duties requirement engagement with other staff members and colleagues, ensure an alignment of timings.

Ensure that the employee takes break times in accordance with the Organisation of Working Time Act. At home the employee is in control of their working time, this does not however permit a departure from the obligation to take breaks.

It is essential that the employee takes care of their physical wellbeing, to include getting up and walking around every so often to alleviate any constraints or physical stresses of working at a non purpose built work environment.

Management will diary and facilitate social check ins to ensure the wellbeing of the employee, feedback on work progress, performance, and any miscellaneous issues arising.

## Policy and Procedure Compliance

The employee is expected to adhere to the normal requirements of attendance, appropriate dress when attending meetings online, the Company Code of Conduct, Social Media, Confidentiality, Employment Equality and Anti Bullying policies, this is a non-exhaustive list. Behaviour is expected to abide by standards of mutual respect, professionalism and best practice.

## Communication and Meeting Arrangements

The Company will use virtual communication tools and applications to communicate during remote working:

- Zoom/Teams/Webex – for video conferencing, meetings and calls
    - Meetings where so occurring will be kept to strict time limits as set out in an agenda circulated prior to the meeting
    - Meetings will be recorded on zoom to facilitate minutes and as a record of decisions made
- Whatapp/Viber – for instant messaging utilizing one to one and group contact and communications
- Email – for all written communication, document circulation
- Dropbox for all sizeable documentation
- Telephone calls on mobile or a land line of the employees nomination

## Cybersecurity and Data Privacy Considerations

Remote working obliges the employee to work from a mobile device. However, we recognise that the convenience of mobile working must be weighed up against the increased risk of losing the data contained on it due to the very nature of its portability and the fact that you are carrying around sensitive company data, or access to such data with the immediate and material security risk for if the data is lost or stolen. Also any entry point into our networks for mobile devices is potentially an entry point for malware and viruses.

Whenever data is transferred from one location to another, it should be pseudonymised and/or encrypted to protect it from being leaked.

Pseudonymisation masks data by replacing identifying information with artificial identifiers and can help protect the privacy and security of personal data.

Encryption obscures information by replacing identifiers with something else.

Pseudonymisation allows anyone with access to the data to view part of the data set, encryption allows only approved users to access the full data set.

Pseudonymisation and encryption can be used simultaneously or separately.

Here are the general guidelines with regard to remote working:

- ensure all laptops used for work purposes are encrypted and that devices are registered with the company and benefit from our mobile security package;
- all personal laptops must have the company security software installed;
- do not use private email (e.g. hotmail) accounts for work purposes;
- you are specifically prohibited from downloading company data to be stored on a personally owned mobile device;
- ensure that you notify your manager and/or IT department in the event that you experience a data loss/theft;
- ensure that you have secured the ability to remotely wipe devices that are lost or stolen;
- ensure that you update your mobile device to avoid any malware or phishing scams;
- ensure that your device has multiple layer passwords that incorporate a mixture of alpha and numerical characters (complex passwords);
- no apps are to be installed onto work related devices without specific advanced permission;
- uninstall apps that are not in regular use;
- you must not dispose of or loan your personal device unless you have verified that it has been securely wiped of all company data;

- your mobile devices must be set to have an automatic locking mechanisms if inactive for a period of time and to wipe the data if the password is entered incorrectly a number of times;
- change your passwords on your mobile devices for work purposes every 90 days;
- be alert to the possibility of phishing emails and unexpected links and files sent by 'friends'. these may be malware;
- the company reserves the right to revoke access to devices if anything of a suspicious nature is considered to occur;
- you must not access company data via any unsecured networks most especially in public places; personal "hotspots" must be utilised as an alternative to a secured network;
- ensure the privacy of your desktop and materials utilised while remote working, ensure that no one has access to work related data, to include returning files and documents to work, having a shredder at home to ensure ongoing shredding of materials so as to avoid leaving them lying around at home,
- file emails promptly and delete unwanted items;
- upon termination of your employment you must deactivate your access to all company related information/access points from your own network and you will be deactivated in so far as possible by the company;
- do not leave your device in for repair without having it first wiped of all company related data;

If you are granted permission to work remotely you are required to abide by all of the content of this policy, to fail to do so may result in disciplinary action up to and including dismissal.

## Insurance

The Company requires that the employee notify their insurance company and have the company's interests noted on the Home Insurance policy.