Remote Working Policy

Introduction

Remote working (previously telecommuting and teleworking) allows employees to work at home, on the road or in a satellite location for all or part of their workweek. Interr considers remote working (incl hybrid working) to be a viable, flexible work option when both the employee and the job are suited to such an arrangement. Remote working may be appropriate for some employees and jobs but not for others. Remote working is not an entitlement, it is not a companywide benefit, and it in no way changes the terms and conditions of employment with Interr.

Related policies

This policy should be read and followed in conjunction with the Hybrid Working Policy and all Information Security policies, including but not limited to Data Protection Policy, Computer & Electronics Policy, Clear Desk and Screen Policy, Mobile Phone, Information Handling, and Information Security Incident Reporting Policy.

Remote working employees must comply with all Interr's rules, policies, practices, and instructions. Any breach will be investigated and may result in disciplinary action taken.

Requirements

A remote working employee must perform work during scheduled contracted hours. Employees may not engage in activities while telecommuting or teleworking – remotely working that would not be permitted at the regular worksite, such as child, elder, or other dependent care. Remotely working employees may take care of personal business during unpaid lunch periods, as they would at the regular worksite.

Employees are expected to maintain a presence with their department/division while working remote. Presence may be maintained by using appropriate technology including but not limited to a computer, email, messaging application, video conferencing, instant messaging, Google sheets, and/or text messaging. The employee is expected to maintain the same response times as if they were at their regular Head Office location and will make themselves available to attend scheduled work meetings as required and/or requested.

Safety

Employees are expected to work in a safe way, conducting regular dynamic risk assessments and aware of their surroundings. As you may be working on your own whilst remote working 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 you do not feel or you have any health and safety or a wellbeing related problem, contact your line manager immediately.

Protection of assets and information

Every member of our organization is entrusted with the responsibility of protecting company assets. We foster a sense of accountability to ensure that every decision and action aligns with our commitment to safeguarding our resources.
Employees are responsible for the security and protection of the equipment, information and assets assigned to them for remote work.

Information technology resources may only be used for authorized business purposes. Personal use should be reasonable and not interfere with work responsibilities. Users are expected to conduct themselves ethically and responsibly in all interactions with information technology resources and be responsible for maintaining the security of their accounts, including passwords and access credentials.

All employees and anyone who has access to the company's sensitive data must follow data protection policies and guidelines to safeguard sensitive and confidential information.

Prohibited Activities:

- Unauthorised Access:
  - Unauthorised access to information technology resources, systems, or data is strictly prohibited.
- Malicious Software:
  - Installing, distributing, or using malicious software, including viruses and malware, is prohibited.
- Unauthorised Sharing of Access Credentials:
  - Users must not share their access credentials or allow others to use their accounts without proper written authorization from the IT department.
- Unauthorised software
  - Employees are not allowed to use or access any software/hardware that's not approved by the company.
- Network Abuse:
  - Engaging in activities that compromise the organization's network integrity, such as unauthorized scanning or hacking attempts, is prohibited.
- Harassment and Discrimination:
  - Using information technology resources to engage in harassment, discrimination, or the dissemination of offensive content is strictly prohibited.
- Illegal Activities:
  - Engaging in any illegal activities through the organization's information technology resources is strictly prohibited.
- Company assets for personal use
  - Watching, downloading, streaming films, series, music etc on company-owned assets is prohibited and cannot be accessed in order so the copyright laws and licencing agreements are not infringed.
- Leaving company assets unprotected
  - Under no circumstance is anyone allowed to leave company assets unprotected by leaving them unlocked when not in use or leaving them in an area where others can have access to it;
- Deliberately exposing equipment to physical or environmental threats
  - Failing to comply with the company information security policies, specifically Computer and Electronics policy and Clear Screen and Clear Desk policies;
- Removing company assets without permission
  - Only staff permitted by the exec board should be able to remove and carry company property around;

Security

The company has location tracking and the ability for remote wiping of devices if and when required.

Consistent with the Company's expectations of information security for employees working at the office, remote-working employees will be expected to ensure the protection of confidential information accessible from misuse whilst remote working (telecommuting/teleworking).

Any media, documents or systems containing sensitive information shall be protected against unauthorized access, misuse or corruption during transportation. Steps include protecting your work equipment, not leaving it unattended, regular password maintenance, or transported in a way that mitigates the risk of theft or loss and stored in a separate folder away from other valuables, including portable equipment and other electronic devices and any other measures appropriate for the job and the environment.

Remote workers must ensure that official records and information are secure and not maintained in a way that would make them available to any other individuals except as appropriate, consistent with Interr's work obligation.

All files, records, papers, or other materials accessed while remotely working are Interr's property. Remote workers employees and their supervisors shall identify any confidential, private, or personal information and records to be accessed and ensure appropriate safeguards are used to protect them.

Employees should not work in any exposed or unsecured areas when handling confidential or sensitive material. Departments may prohibit employees from printing confidential information in remote working locations to avoid breaches of confidentiality. Employees may not disclose confidential or private files, records, materials, or information, and may not allow access to Interr's networks or databases to anyone who is not authorized to have access.

Any suspected data breach containing sensitive data or unauthorized access to or disclosure of official information or systems, or a loss of any company equipment must immediately be reported to the remote worker's supervisor and the and the IT System Administrators who will notify the Chief Information Security Officer. Such unauthorized access or disclosure, including the release of confidential information or the personally identifiable information of Interr or Interr's staff or customers, which happened due to the remote worker's neglect, will be addressed through disciplinary actions.

Remote workers must protect and safeguard files, documents, equipment, and other materials transported back and forth between the official work site and the alternate work site.

Remote workers shall protect official records and documents from unauthorized disclosure or damage and shall comply with all established policies and procedures regarding such matters.

Remote workers must also take the following specific precautions:

- Only take confidential information offsite when authorized in advance by their immediate supervisor/manager.
- Never transmit confidential information from work e-mail to any personal e-mail addresses or text messaging services (e.g., icloud.com, aol.com, yahoo.com or g-mail.com).
- Securely store all hard copy documents or office media so that others cannot access it.
- Do not communicate confidential information where others can listen.
- Remote worker must not throw away Company's sensitive information in hotel wastebaskets or other publicly-accessible trash containers. They must be uploaded to Interr's secure systems first and shredded in the designated shredding bins at the official work site.

Under no circumstance may the remote worker use their personal devices for work related use. Only approved and company given property should be used for such purpose. Remote worker should switch off and secure any computer being utilised to conduct official business when not in use, consistent with the company policies and procedures.

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