

Remote Working

14 September 2021

Contents

Remote Working		
1.0	Introduction	3
2.0	Scope and definitions	3
3.0	Eligibility for remote working	4
4.0	Standards for Remote working	4
5.0	General Provisions	4
5.0.1	Converting to remote working	4
5.0.2	Employees requesting to work remotely	4
6.0	Employment Conditions	5
7.0	The concept of 'contact hours' and 'core hours'	5
8.0	Registering attendance for remote workers	6
9.0	Right to Disconnect	6
10.0	Remote workspaces	6
11.0	Professional Standards	6
12.0	Data Protection	7
13.0	Privacy	8
14.0	Equipment	8
15.0	Data connectivity for all remote workers	8
16.0	Health and Safety	9
17.0	Organisation of Work	9
18.0	Training & Career Development	9
19.0	Job suitability	9
20.0	Employee Suitability	10
21.0	Remote working agreement	13

Appendices

Appendix 1

Application for remote working on an individual basis

1.0 Introduction

The drive towards more innovative working arrangements is being spurred by the huge advancements in technology. This is facilitating a transition to new realities, fostering opportunities for digital working flows and developing new opportunities. Moreover, apart from consolidating the Public Service's stance towards work-life balance itself a leader in the field - the Public Service is adopting solutions which are also beneficial to the wider community.

The purpose of this policy is to set up a formal framework for the administration of remote working in the Public Administration of Malta.

This policy will come into effect as from 1st October 2021. There will be a transitional period of 18 months starting from the effective date of this policy. During the transitional period, the necessary investments in capital equipment, technology, and training of staff are to be carried out. The policy will become fully in force as from 3rd April 2023.

2.0 Scope and definitions

i. Scope

This policy applies to Public Officers within the Public Service performing job roles classified by the Head of Department as compatible with the concept of remote working.

ii. Definitions

a. Remote working

Remote working is a way of doing work which provides employees with full flexibility in the locations other than their formal office, from home, an alternative office closer to home, or at any other location on a regular basis.

b. Remote workers

A remote worker is any employee carrying out remote working duties as defined above.

c. Head of Department

For the purpose of this policy, the term Head of Department refers to the Permanent Secretary or to any other officer to whom power to authorise remote working has been delegated.

d. Clients

Clients may be internal and/or external to the Public Service.

3.0 Eligibility for remote working

Employees whose job performance and skills, as well as the nature of their job, are suitable to be carried out away from traditional office set-ups, may request to engage in remote working. Employees on a trial basis are eligible to apply for remote working subject to the approval of the Head of Department. The Head of Department may indicate a shorter period when the employee on trial can apply for remote working.

Conversely, new recruits engaged from outside the public service are not eligible to work remotely while on probationary period.

4.0 Standards for Remote working

The Head of Department must ensure that the minimum standards concerning the IT aspect, Training and Logistics, amongst others, and which are established by this policy are in place prior to switching to remote working.

5.0 General Provisions

Remote working is at the discretion of the Head of Department and in considering remote working arrangements, the Head of Department shall consider both the operational requirements of the department and the service offered to its clients.

The Head of Department shall have the right to terminate a remote working arrangement after giving fifteen (15) working days' notice. The foregoing notice period does not apply whenever the arrangement is terminated due to failure to meet the desired standards and workloads, or if it results that the provisions of this policy are abused. In such cases, the working arrangement shall be terminated with immediate effect without prejudice to any further action.

5.0.1 Converting to remote working

The Head of Department may opt to switch a particular section, department, or function, partly or entirely to remote working whereby all employees within the section, department or function are obliged to work remotely within the conditions outlined in this document.

In such circumstances the following procedure is to apply:

1. The respective Head of Department shall give ten (10) working days' prior notice to employees within the section, department, or carrying out a particular function, clearly identifying the grades and roles which will be switching to remote working;
2. Should circumstances arise whereby an employee has reasons not to work remotely, the employee shall notify the Head of the Department in writing through the Head of Section. The Head of Department shall then assign the employee to another section or Department not affected by remote working within the same Ministry.

5.0.2 Employees requesting to work remotely

Public Service employees may, on their own initiative, submit a written request to their Head of Department, through their immediate superior, to switch to remote working. In their request, employees must confirm their understanding of this document and underline the necessary skills to work remotely as per section 18.0 of this policy document.

The Head of Department shall verify the job suitability in line with sections 19.0 and 20.0 of this policy and shall, within eight (8) working days from receipt of the request, take a decision on the request submitted.

6.0 Employment Conditions

The same rights guaranteed by relevant legislation, policies, and collective and sectoral agreements shall continue to apply to all employees irrespective of whether they have a remote working agreement or not.

Similarly, all employees are required to attend and/or participate in all the necessary meetings, work-related events, seminars, conferences, training sessions, and other activities which demand their physical presence as may be requested by management from time to time.

To maintain effective communication, remote workers are encouraged to work as part of a team and are advised to communicate with their manager and/or colleagues on a regular basis. On the other hand, the Head of Department, or their delegate, is responsible for maintaining a healthy working relationship amongst their employees, whether they are working remotely or not. The Head of Department or their delegate shall physically meet, at least once every fortnight, with all remote workers at any location. Such meetings may be held with the entire remote working team or with as many individuals as may be logistically feasible.

Remote workers must agree not to leave vacation leave accumulate towards the end of the calendar year. Absences for annual leave, special leave and sick leave shall be accounted for on the basis of a normal working day of summer/winter hours. Employees shall provide a vacation leave planner in terms of para 3.1.9 of the PSMC.

7.0 The concept of 'contact hours' and 'core hours'

Core hours

Core hours will be established by the Head of Department with a view to facilitating the day-to-day operations of remote working teams. Remote workers shall remain available throughout the core hours as part of their official working hours. In case of employees working on a reduced schedule, the total amount of available contact hours per day shall be calculated pro-rata.

Contact hours

Contact hours will be established by the Head of Department as set hours when remote workers may be requested to be available. The contact hours shall be established within the officer's normal working hours. Notice to remote workers to remain available during the set contact hours must, as much as possible, allow for a prior notice of twenty-four (24) hours.

During the contact hours and core hours, employees are expected to remain accessible by phone, e-mail, and any other official means of communication, and the provisions of Directive 4-1 are to be adhered to throughout. Vacation leave may be availed of during core and contact hours upon approval.

The hours set to establish the core and the contact hours collectively shall be based on an annual average of forty (40) hour week schedule. The core and contact hours for employees working on a reduced schedule timetable shall be based pro-rata.

8.0 Registering attendance for remote workers

Remote workers shall make use of a centrally-approved electronic Attendance Verification System (AVS) to register their attendance. Workers shall be allowed at any time to request and obtain the record of their working times.

9.0 Right to disconnect

The policy embraces the right to disconnect principle and grants workers with the right to be able to disengage from work and refrain from engaging in work-related electronic communications, such as emails or other messages, during non-core and contact hours.

In cases, however where a contract of employment specifies otherwise, or a worker benefits from an allowance to cover an irregular schedule of work, this principle shall not apply.

10.0 Remote workspaces

Remote workspaces shall be available to employees on a first-come-first-served basis. Employees may opt to work away from these identified remote workspaces. However, set standards are to be observed in all circumstances.

11.0 Professional Standards

All employees, whether working remotely or otherwise, are bound by the quality service standards established by the Public Service. The rules, regulations, directives, and policies applicable to public employees are to be strictly adhered to when working remotely. These guidelines are to be read in conjunction with the Code of Ethics for Public Employees and the Professional Standards issued through the PSMC.

1. Employees working away from the office are to ensure that appropriate office attire is worn when making video calls.
2. Employees are expected to be connected in time for any online meetings scheduled. Video calls should be held in quiet places. Headphones should be used in order to ensure confidentiality and the 'raise hand' function should be used, when necessary, to minimise disruption. Cameras should be turned on and microphones should be kept muted unless the participant is speaking.
3. To maintain a professional image of the Public Service, it is important that when making video calls, backgrounds are blurred. Alternatively, if employees are not working from an office setup, they can use corporate backgrounds. Inappropriate and unprofessional backgrounds are not allowed and are censored.
4. Whenever an employee needs to record a call, s/he shall ensure that the other person/s taking part in the same call are informed beforehand and shall only proceed with the recording if all parties give their consent to the recording. No calls shall be recorded without the consent of all persons taking part in the same call. Recorded meetings shall be saved in terms of the policy concerning information retention. Disciplinary action will be taken against employees who do not adhere to these provisions.
5. During video calls employees shall ensure that they are following what the other participant/s is/are saying, and should avoid carrying out other tasks such as reading e-mails, browsing, or eating.

6. Employees are to ensure that confidentiality and data protection are maintained at all times. Confidential phone/video calls and meetings shall take place in locations that may not, in any way, compromise confidentiality or lead to leakage of information. Likewise, great care is to be taken to make it impossible in any way for third parties to view, read, or come into possession of official and confidential documents.
7. Employees shall keep any communication system installed on their computer on during the established available contact hours to ensure that they can be easily reached.
8. When communicating with clients, the quality service standards stipulated by Directives 4-1 and 8-1, including the established timeframes, are to be adhered to at all times.
9. Active communication is to be maintained at all times to avoid alienation and disassociation from the rest of the team.
10. If an employee is unable to work owing to sickness, the PSMC sick leave provisions, as well as any internal policy on the communication of sick leave, shall apply.

12.0 Data Protection

Ministries are responsible for taking all the appropriate measures in order to ensure that any data used by the remote worker in connection with their working activity is fully protected. The Head of Department or their delegate should indicate to the employee the applicable rules and regulations concerning data protection. It is the employee's responsibility to comply with these rules and regulations, and in case of any breaches the remote working agreement may be terminated without prejudice to further action.

The procedures applicable for notifying a data breach shall be applied as per general rules of the data protection act. In such instances, an employee who becomes aware of a data breach shall immediately notify the direct superior for further referral to the Data Controller.

The Data Protection Act¹ refers to the controller's responsibilities for the fair and lawful processing of personal data, and that such data should not be kept for a period longer than necessary. Therefore, in order to safeguard the requirement defined in the GDPR, the total management of the data security is to be considered by the Head of Department or their delegate before any data is passed to the remote-working employees for processing.

The security of equipment, assets, information, confidentiality, and copyright should be in accordance with Government's relevant policies. Employees shall ensure the protection of any work-related and client information accessible from remote places. Measures for security include the use of locked file cabinets and desks, regular password maintenance, and other appropriate measures consistent with the nature of the work.

Remote workers shall ensure that other household members or friends do not have access to work related documents, personal and/or confidential data as defined by the Data Protection Act.

The Head of Department or their delegate shall inform employees of their responsibility to abide by the Government Policies and Standards² on MAGNET connectivity, e-mail and Internet use policies, use of software such as anti-virus and spam control, and any applicable security and technical issues as advised by MITA, being the provider of technology services to the Government.

¹ The Data Protection Act (Chapter 586 of the Laws of Malta) may be accessed on www.legislation.mt

² Documents include: Connectivity to MAGNET Policy (v2.0); Connectivity to MAGNET Directive (v1.0); Connectivity to MAGNET Standard (v1.0); Information Security Policy; Minimum Information Security Directive (v2.0); all of which may be accessed on <https://mita.gov.mt>

The European Directive on Privacy and Electronic Communications (2002/58/EC) imposes special rules concerning the processing of personal data and the protection of privacy in the electronic communications sector. Heads of Department authorising remote working should likewise familiarise themselves with this Directive, and are responsible for ensuring that remote working employees are aware of the Articles that are deemed relevant to their work.

13.0 Privacy

The Head of Department must ensure that whilst the privacy of employees working remotely is respected, the security norms are in place. The Head of Department (*or their delegate*) is to ensure that remote employees' privacy is respected, whilst also ensuring that the security norms are in place. Any monitoring systems, such as the centrally approved electronic Attendance Verification System, must be proportionate to the objectives to be achieved.

Employees should be advised in cases where their activity is being monitored. This includes cases of the utilisation of key-logging software where all activity on the employee's computer can be tracked and recorded, or where the employee's computer is being controlled remotely.

The GDPR and Data Protection Act (Chapter 586 of the Laws of Malta) may be accessed on www.legislation.mt

14.0 Equipment

The Public Service is responsible for providing and maintaining the equipment necessary for remote working. Ministries are to ensure that such equipment is covered by a proper data protection impact assessment and a complementing data protection policy.

Any physical damage sustained to the equipment should be immediately reported by users to their superiors. Hardware used for remote working will be governed by the relevant policies on the use of ICT in Government.

The enabling equipment for remote working shall include a centrally managed mobile device with secure data connectivity to allow for the installation of IT software approved centrally by the competent authority. Software should include, but is not limited to, attendance verification systems, a secure application to access the remote workspaces, a task management solution, a booking facility solution, access to cloud PABX for data calling, and any other software that may be required from time to time.

15.0 Data connectivity for all remote workers

Remote working will provide a viable means of data connectivity to all employees by providing a secure third-party data plan through Government-controlled equipment. Data communication through this tool will allow remote workers to operate standard office applications.

16.0 Health and Safety

The nature of remote working is very flexible and cannot be associated with any particular working location. Creating fixed locations goes against the fundamental principles of remote working and will undermine agile working practices.

Since remote working should promote employees' mobility, the employer's responsibility for the health and safety of remote workers is only limited to the official remote workspaces and cannot be extended to any other remote workstation in accordance with the Occupational Health and Safety Authority Act (Cap. 424), and collective agreements.

Remote workers shall take reasonable care of the remote equipment tools and are to examine such equipment from time to time, with a view to ensuring that they remain functional and safe.

17.0 Organisation of Work

Arrangements should be put in place to ensure that all employees have the same access to Government information as their office-based colleagues.

All internal communications such as memos and newsletters are to reach remote workers promptly by means of the formally established digital channels.

18.0 Training & Career Development

The Institute for the Public Services (IPS) shall be responsible for providing training to managers and non-managers on how to professionally manage and sustain a remote working team.

The training programme for managers addresses management and leadership skills for a remote working environment, awareness on software and applications of ICT Tools for effective remote working, and data protection issues.

The training programme for non-managers comprises working effectively within a remote working environment, awareness on software and applications of ICT tools for effective remote working, and data protection issues.

Before engaging in remote working, employees shall provide evidence that they have successfully attended IPS training to help them acquire the necessary skills and knowledge required to work remotely, with a view of ensuring that the level of service offered to the client is not negatively affected.

Remote working employees shall have the same access to other training, which may be given outside the available contact hours, career development opportunities and promotions and are subject to the same appraisal policies as employees working from the office.

19.0 Job suitability

Jobs suitable for remote working include those involving a high degree of information-processing that also have clear objectives and measurable outputs, and require minimal supervision. The impact on the service offered to clients, as well as on the employee when delivering the service, should be taken into consideration.

Jobs that require employees' ongoing physical presence and jobs which require face-to-face contact with the public and/or other staff members are not suitable for remote working.

20.0 Employee Suitability

In order for an employee to conduct their duties from remote locations successfully, the employee must possess, amongst others, the following traits and skills:

- a. Ability to work independently and without constant supervision;
- b. Competence in time management skills;
- c. Excellent communication skills;
- d. Ability to work in a team; and
- e. ICT literacy skills

21.0 Remote working application and agreement

An individual remote working agreement is valid for a period of twelve (12) months, which may be renewed on a yearly basis. Employees should apply for remote working by clicking [here](#). The template provided at Appendix 1 is only intended for information purposes. Guidelines on the application of remote working on individual basis can be found [here](#).

Approved applications for remote working shall be sent to the Director responsible for the HR/People Management who shall in turn inform IPS for training purposes. Employees who have successfully completed the remote working training programme provided by IPS shall inform the respective Director responsible for the HR/People Management that they have completed the training and provide proof thereof.

After having verified that the training has been successfully completed the Director responsible for the HR/People Management shall conclude the Remote Working agreement at Appendix 1 with the employee, within (3) working days from the date that the employee provides proof that the training has been completed successfully. The Director responsible for HR/People Management shall inform the employee's Head of Department of the date when the employee shall start working remotely. Employees shall not start working remotely prior to the finalization of the agreement with the respective Director responsible for HR/People Management.

Departmental and/or section arrangements are indefinite and at the discretion of the Head of Department.

Appendix 1

APPLICATION FOR REMOTE WORKING ON AN INDIVIDUAL BASIS

Attention all applicants- Any false statement, misrepresentation, or concealment of material fact on this form or any document presented in support of this application may constitute grounds for disciplinary action.

Once endorsed by all parties, this Application constitutes the remote working agreement between the employee and employer as indicated in the Remote Working Terms & Conditions.

Date of request: _____

SECTION 1: APPLICANT'S DETAILS (to be completed by the applicant)

Name:	ID Card No:
Surname:	Office Tel:
Ministry:	
Department/Directorate:	
Grade/Position:	
E-mail:	

SECTION 2: REQUEST

Remote Working agreement is being requested for a period of one year. The commencement date of remote working shall be determined by the Director responsible for HR/People Management after the successful completion of the training provided by the IPS.

The applicant requires the following training (to be indicated by the Director of the applicant):

Remote Working for Employees

Managing Remotely

SECTION 3: CORE AND CONTACT HOURS (as agreed between Director/Head of Department and Applicant)

CORE HOURS: Core hours should be based on an annual average of a forty (40) hour week schedule. Remote Workers shall remain available at their relative location of work throughout the core hours as part of their official working hours.

In case of employees working on a reduced schedule, the total amount of available contact hours per day shall be calculated pro-rata.

Monday	Tuesday	Wednesday	Thursday	Friday

CONTACT HOURS: Contact hours will be established by the Head of Department as set hours when remote workers may be requested to be available. Notice to remote workers to remain available during the set contact hours must, as much as possible, allow for a prior notice of twenty-four (24) hours.

Monday	Tuesday	Wednesday	Thursday	Friday

SECTION 4: ENDORSEMENTS

Employee

Full Name:

Signature:

Date:

Director/Head of Department

Full Name:

Signature:

Date:

Recommended []

Not Recommended [] (if not recommended please provide reason)

Permanent Secretary

Full Name:

Signature:

Date:

Approved []

Not Approved []

(if not approved please provide reason)

Director responsible for HR/People Management

(The details of employees whose application for remote working has been endorsed by the Permanent Secretary are to be submitted to IPS at ips.gov.mt for training purposes. This section to be completed after the employee provides proof that they successfully completed the IPS training.)

The employee has successfully completed the IPS training on / / and can start working remotely with effect from / / .

Full Name:

Signature:

Date:

The information supplied in this application form shall be used exclusively by the employing Ministry for record keeping and verification purposes. Personal information provided on this application form is protected, and used in accordance with the provisions of the Data Protection Act.

SECTION 5: REMOTE WORKING TERMS & CONDITIONS

The Terms & Conditions listed hereunder apply to employees hereinafter referred to as 'remote worker' who are entering into a remote working arrangement with their employing Ministry/Entity.

Prospective remote working applicants should read all terms & conditions before filling in the application for remote working which constitutes of the remote working agreement between the employee and employer.

This agreement is valid for a period of one year unless organisational circumstances arise whereby the employee's Head of Department converts the employee's respective Department/Section/Function to remote working in terms of the Remote Working Policy. In such cases, this contract shall be terminated with effect from the date that the whole department/section/function converts to remote working.

1. The terms of remote working are based on the policy principles outlined in in the Remote Working Policy Document which document may be accessed online and whereby the employee confirms understanding thereof.
2. Remote Working is based on a voluntary agreement between the employee and the employing Ministry.
3. Termination of the remote working agreement can be instigated at any time by either party by giving fifteen (15) working days' notice in writing. The remote worker's failure to meet the agreed standards and workload entails immediate termination of remote working.
4. The employee is expected to remain accessible by phone, email and any other official means of communication during the contact and core hours.
5. The remote worker is subject to the same working conditions in terms of responsibilities, liabilities, policies, employment conditions and all other legislation, regulations, determinations, and code of conduct etc. that are applicable at the central workplace. The employee and Director/Manager are to agree in advance on the deliverables as happens with employees working at base.
6. The remote worker will still be considered as a regular employee and shall be eligible to participate in all activities and enjoy the same benefits as any other employee not on remote working. In the same manner a remote worker will still be bound by the policies, rules and regulations of the employer and is liable to these in the same manner as any other employee.
7. The employer shall be responsible for providing and maintaining the equipment necessary for remote working which are covered by a proper data protection impact assessment and a complementing data protection policy. The remote worker is to be properly instructed in the safe use of the equipment prior to entering into a remote working agreement.
8. Any physical damage sustained to the equipment should be immediately reported by the users to their superiors. Hardware used for remote working will be governed by the relevant policies on the use of ICT in Government.
9. The employee should attend compulsory training session/s provided by the Government on remote-working and ICT tools.
10. All equipment provided by the employer shall remain the property of the employer and the remote workers is bound by all policies and regulations related to such matters as applied in the central workplace. Any security arrangements for equipment and assets and all procedures for securing the confidentiality, protection for information and intellectual property therein are to be in accordance with organisational policy or practice. If a policy is not in place it is the remote worker's responsibility to take measures as would be taken

in a non-remote working environment, including the physical securing of equipment and assets, to protect the interests of the employer.

11. The remote worker is bound by regulations governing use of ICT in Government. All relevant policies are to be observed irrespective of where the remote worker is working and whether the equipment being used for remote working has been provided by the employer or is the employee's own.
12. The equipment used for remote working will be used according to standards and security measures conformant to Government policies and recommendations. By entering into a remote working agreement, the employee is consenting to all reasonable methods of surveillance by the employer to ensure the proposer performance by the employee of the duties of employment.
13. It is to be ensured that work deliverables are monitored and it is the responsibility of the remote worker to adhere to all the reporting mechanisms which may be laid down by the employer.
14. The employer is responsible for the provision and maintenance of equipment. An agreed list of equipment is to be attached to the remote working application and signed by the employee and the Director/Manager. Any changes to this list shall be made in writing and signed by both parties.
15. The remote worker is responsible to take reasonable care of all equipment provided and should periodically examine it to ensure that the equipment remains functional and safe to him/her and other family member or visitors. The remote worker shall not make any modification to the equipment other than with the consent and under the supervision of the employer. Furthermore, the employee is liable for any damage caused due to negligence on his or her part.
16. In order to ensure work continuity, whenever any equipment requires repairs, the remote worker should accept any temporary arrangement provided by the Head of Department. This arrangement shall remain in force until such time as the equipment's functionality is fully restored.
17. The type of work, results measurements, contact and working arrangements are to be agreed to between the employee and the Head of Department. The Head of Department through the respective Director responsible for People Management, should endorse any other proposed changes to the conditions of employment. In case of disagreement, the changes should be endorsed by the respective Permanent Secretary. These arrangements should be documented, signed by both the employer and the remote workers an attached to the remote working application. Any changes to these arrangements should be agreed to and signed by both parties. A copy of the remote working application is to be kept by the employee and another copy inserted in the employee's personal file.

