REMOTE WORKING POLICY

Title	Remote Working Policy
Owners	Office of Performance Management, Office of Information Security
Version	1.1
Issue date	March 2020
Next revision due	February 2023

Contents

1 MANAGING THE POLICY

1.1 Compliance

a) All staff, members and contractors or others with access to the Charity's information must comply with this policy.

b) Anyone who is found to have breached this policy could be subject to disciplinary procedures and serious breaches of this policy could be regarded as gross misconduct.

c) If you do not understand the implications of this or how it may apply to you, seek advice from Office of Performance Management.

1.2 Equality and Diversity

Every policy must consider equality and identify any potential barriers or discrimination faced by people protected by equality legislation.

2 INTRODUCTION

2.1 For the purpose of this policy, the term remote working applies equally to home, flexible and mobile working.

2.2 To enable the Charity maximize its employees' effectiveness and productivity, but at the same time giving more flexibility in their working lives, the Charity is committed to supporting remote working.

2.3 The Charity, in support of remote working, will provide the environment and tools to reap the benefits of adopting flexible working practices that meet the needs of the organization, the team and individuals. This will maximize our ability to provide the highest quality of programme delivery whilst at the same time managing our operating costs. This in the long term may contribute to better use of office space and our car parking facilities. The Charity believes that having high quality, motivated, and highly effective staff is the best route to achieving its goals.

2.4 The Charity will ensure that all users who work from home or remotely are aware of the acceptable use of portable computer devices and remote working opportunities. Portable computing devices are provided to assist users to conduct official Charity business efficiently and effectively. This equipment and any information stored on it should be recognized as valuable organizational information assets and must be safeguarded appropriately.

2.5 The Charity is committed to its duty to fulfill the requirements of the Equality Act 2010. Where reasonable adjustments are already made at employee display screen workstation, such as ergonomic and/or personalized equipment, that same help, support and protection shall be afforded to home workers.

3 PURPOSE AND OBJECTIVES

3.1 The purpose of this policy is to establish the standards, working practices and supported configurations of remote working solutions.

3.2 The Charity aims to recruit and retain key personnel with the necessary skills and knowledge to assist in meeting its overall objectives. The Charity therefore supports remote working where an employee's effectiveness, productivity and efficiency can be enhanced by working from home or flexible locations on specific projects, or for other specific reasons where possible and practical. Remote working can also be a benefit to the employee allowing them to have flexibility for an equivalent or enhanced service to the Charity, regardless of location around the world.

3.3 This Charity is committed to adopting a flexible approach to working arrangements and remote working may, therefore, be part of the employees working pattern or may be carried out as and when required or as is deemed appropriate.

3.4 Remote working has a number of benefits for the employee and employer. The employee gains greater flexibility of working times, time and cost savings on commuting and can have a quieter work environment in which to undertake their work. Remote working supports the Charity's environmental objectives by reducing unnecessary car travels and freeing up office accommodation spaces.

3.5 Remote working must not be seen as an alternative to making usual childcare/dependant/carer arrangements, any arrangements that the member of staff would require to have in place to enable him or her to attend the workplace must remain in place throughout the remote worker's hours of work.

4 SCOPE

4.1 This policy applies to all the Charity's Board of Directors, members of staff (including temporary and contract), partners, contractual third parties and agents of the Charity who have access to the Charity's information, information systems or ICT equipment and intend to store any information on removable media devices.

4.2 It is appreciated that this concept may not be suitable for many types of work, but a wide range of posts can be considered for remote working, especially, within the Matrix Headquarters system.

4.3 The one area not suited for remote working is when the post requires a high element of continued face-to-face public/client contacts such as country and field program operations, including emergency and humanitarian responses.

5 TWO TIER SYSTEM

5.1 This policy is split into two separate categories:

a) **Hot Desking** - where the employee wishes to work at home on an ad-hoc basis, which is to the benefit to the employee allowing flexibility and meets the business needs, whilst also minimizing the need for on-site accommodation.

b) **Home or Remote Working -** Employees who may apply under the Charity's Flexible Working Regulations, to work from home and who are contracted to work a certain number of hours at home as part of their contract.

6 DEFINITION

6.1 This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of the Charity's ICT equipment and personal ICT equipment when working on official Charity business away from the Charity's premises (i.e. working remotely).

6.2 The policy also applies to all users' use of the Charity's ICT equipment and personal ICT equipment to access the Charity's information systems or information whilst outside the United Kingdom.

6.3 Portable computing devices include, but are not restricted to, the following:

a) Laptop computers
b) Tablet PCs
c) Palm Pilots
d) Mobile phones including Smart phones
e) Text pagers
f) Wireless technologies

6.4 **For both Hot Desking and Remote working,** it is essential that those undertaking work from home or flexibly are able to make available a room or area of their home for use as an office/working area. The employees work location, however, will remain at the Charity's designated Office as included in the terms of their contract of employment.

7 HEALTH AND SAFETY

7.1 Remote working

7.1.1 All employees who work at home have duties under the Health and Safety at Work Act in the same way as other employees. Managers will be responsible for ensuring appropriate risk assessments are undertaken. The Office of Performance Management has details of safety checks to be carried out. For an employee who is contracted to work at home, remote working will only be possible where;

a) An appropriate risk assessment has been undertaken; and

b) It has been established that such working will not unreasonably impact on the employee's health and safety; and

c) There are suitable facilities at the employees home to effectively carry out the role; and

d) Effective mechanisms for communication and support are in place.

7.1.2 A Remote Working Risk Assessment Checklist must be completed, and further assessments may be carried out to ensure the employees' health and safety.

7.2 Hot Desking

7.2.1 Where the employee is only working from home on an ad-hoc basis, the employee may carry out a self-assessment at home, and report on it to the Office of Performance Management.

8 COMPUTER EQUIPMENT

8.1 There are several ICT solutions to achieving a suitable working from home environment. The solution installed will largely depend on the type and quantity of work that the employee will be undertaking at home. This decision will be made in consultation between ICT and the Manager, in accordance with the budget of the Service Area.

8.2 Special attention will be paid to any requirement to use or access information that is deemed OFFICIAL-SENSITIVE or SECRET in accordance with the UK Government's Security Classifications and any restrictions imposed under relevant statutory compliance rules.

8.3 Please see Appendix 1 for details of ICT definitions.

8.4 It is encouraged that if the employee only wishes to work from home on an ad hoc basis and it is for their personal benefit to do so, that they use their own computer equipment, subject to the employee being able to connect to the Charity's remote access website.

8.5 In certain circumstances, it may not be technically feasible to provide the ICT facilities required for an employee to carry out their role effectively from home. In these instances, the Service Area Manager will be advised by ICT Services, Office of Information Security, in liaison with the employee.

9 ICT SUPPORT

9.1 If the employee uses their own computer equipment, they will be responsible for any repairs or technical support. Charity equipment will be repaired by ICT Services, Office of Information Security.

10 TELEPHONE

10.1 Where appropriate, the Charity will provide access to a telephony system. If the employee uses their own telephone line, charges for business calls (excluding line rental) will only be reimbursed if clearly identified on an itemized bill and agreed with the manager.

11 OTHER EXPENSES

11.1 If the employee has requested to work from home, expenses for heating, lighting etc., will not be reimbursed by the Charity.

11.2 Stationery will be provided by the Charity, but employees should notify their line manager of all stationery taken out of the office.

12 SECURITY

12.1 The Charity's Information Security Policy must be complied with at all times

12.2 **For both Hot Desking and Remote working,** employees are responsible for the security of all data, whether held on disc or encrypted memory stick or paper, and must ensure it is stored securely to maintain confidentiality of information from members of the family or visitors.

12.3 Sensitive material or personal data must be disposed of by recognized methods using office based shredding equipment or other approved means. Further information on data protection is held within the Charity's Data Protection Policy.

12.4 It is the user's responsibility to ensure that the following points are adhered to at all times:

a) Users must take due care and attention of portable computer devices when moving between home and another business site/office;

b) Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas;

c) Users will not install or update any software onto a Charity owned portable computer device;

d) Users will not install any screen savers onto a Charity owned portable computer device;

e) Users will connect with a wired connection wherever possible. Where a wired connection is not possible and a wireless connection is used, this should be a secure connection. Personal, OFFICIAL-SENSITIVE or SECRET data should **not** be accessed via unencrypted wireless connection;

f) Users will not install any hardware to or inside any Charity owned portable computer device, unless authorized by the Charity's ICT Services, Office of Information Security;

g) Users will allow the installation and maintenance of the Charity's installed Anti-Virus updates immediately;

h) Users will inform the ICT Services Helpdesk of any Charity owned portable computer device message relating to configuration changes;

i) Business critical data should be stored on a Charity network drive and not held on the portable computer device;

j) All faults must be reported to the ICT Services Helpdesk;

k) Users must not remove or deface any asset registration number;

l) User requests for upgrades of hardware or software must be approved by a Business Unit Manager with financial authorization. Equipment and software will then be purchased and installed by ICT Services;

m) No family members may use any Charity provided equipment. The Charity provided equipment is supplied for the staff members' sole use;

n) The user must ensure that reasonable care is taken of the Charity's equipment supplied;

o) The user should seek advice from the Charity before taking any Charity supplied equipment outside the United Kingdom. The equipment may not be covered by the Charity's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel;

p) The Charity may at any time, and without notice, request a software and hardware audit and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit;

q) Any user who chooses to undertake work at home or remotely in relation to their official duties using their own ICT equipment must understand that they are not permitted to hold any database, or carry out any processing of OFFICIAL-SENSITVE or SECRET information relating to the Charity, its employees or clients. **Under no circumstances** should personal, OFFICIAL SENSITIVE or SECRET information be emailed to a private non-Charity email address. For further information, please refer to the Charity's Email Policy; and

r) Any user accessing or using OFFICIAL-SENSITIVE or SECRET information, must only use Charity-owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely. Connection for this device must be with a wired connection and no unauthorized wireless connections must be used.

12.5 Remote and Mobile working arrangements

12.5.1 Users should be aware of the physical security dangers and risk associated with working within any remote office or mobile working location.

12.5.2 Equipment should not be left where it would attract the interests of the opportunist thief. In the home, it should also be located out of sight of the casual visitor. For home working, it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use by either locking away in a cupboard or drawer or by locking the device to the desk (suitable locks can be provided or recommended by ICT Services).

12.5.3 Users must ensure that access/authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. Removable media devices and paper documentation must not be stored with the portable computer device. Paper documents are vulnerable to theft if left accessible to unauthorized people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing OFFICIAL-SENSITIVE or SECRET information must be shredded to required standards (DIN Level 4, Cross cut [1.9mm x 14mm])

12.6 Anti Virus Protection

12.6.1 ICT Services will deploy an up-to-date Anti Virus signature file to all users who work away from Charity premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every two weeks to enable the Anti Virus software to be updated.

12.7 Access Controls

12.7.1 It is essential that access to all personal, OFFICIAL-SENSITIVE or SECRET information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password or user login controls.

12.7.2 Portable computer devices should be switched off, logged off, or keyboard locked when left unattended, even if only for a few minutes. All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL-SENSITIVE or SECRET data held on the portable device must be encrypted. A sufficiently secure remote access mechanism must be configured to allow remote users access to the Charity's systems if connecting over Public Networks, such as the wireless Internet.

12.7.3 Two separate means of authentication (i.e. username/password and PIN Number or Microsoft Two factor authentication app) must be used when accessing the Charity's network and information systems (including Outlook Web Access or Office 365) remotely via both the Charity owned and the non-

Charity owned equipment. Access to the Internet from the Charity owned ICT equipment should only be allowed via an onward connection (i.e. you must connect to the Charity's network first then access the Internet)

12.7.4 As compliance criteria on the Charity become more complex, the ICT Service may need to apply further security controls from time to time. Any such changes will be communicated to all staff with access to a Charity-owned computer. Such security controls may be applicable to the Charity owned and privately owned devices, should the user not wish their privately owned device to be subject to security controls then that device may not be allowed to connect to the Charity network or access any of the Charity's information.

13 HOURS WORKED

13.1 **Hot Desking -** For employees who work at home on an ad hoc basis, the number of hours to be worked at home will be agreed and monitored by the employee's line manager.

13.2 **Remote working -** The hours may be stated within the employees contract of employment, or if a more flexible arrangement has been specified, the number of hours to be worked at home will be agreed and monitored by the employee's line manager. For remote working purposes, the Line Manager can agree with the employee when they will be "at work" and it may be possible for some work to be completed in the evenings or at weekends.

13.3 Employees who, as part of their standard working pattern, work from home for a significant amount of time may not be included in the Charity's flexible working hours' scheme. This will be at the discretion of their line manager and with the agreement of the Head of Personnel Service, Office of Performance Management.

13.4 Support through the ICT Helpdesk will operate during business hours only. No ICT support is provided outside of these hours. Calls for ICT support can be handled by the Charity's contact centre.

APPENDIX A – Definitions

ADSL / VDSL	The technology which allows a domestic phone line to be used for broadband service.
Broadband	High speed Internet – usually provided by ADSL(2),VDSL(2) or via cable or network providers.
"Ultra Lite Teleworking"	(Just as many people no longer have a Charity-provided mobile phone, but use their own mobile phones – with re-charges to the Charity if and when appropriate), many people now have their own private home computers and their own home broadband connections.
"Full Teleworking"	Full VPN access with all the necessary routers and Charity-provided laptops, VoIP phones, etc.
VPN	The home equipment essentially becomes part of the Charity's network, using technology called "virtual private network".

Registered Office:

Population International,
Cariocca Business Park,
2 Sawley Road,
Manchester, M40 8BB
England.