Home and Remote Working Policy

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

DMRC 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 as is appropriate.

DMRC understand that benefits are;

- greater flexibility of working times
- time and cost savings on commuting
- have a quieter work environment in which to undertake their work
- environmental objectives by reducing unnecessary car travel
- freeing up office accommodation

Remote working must not be seen as an alternative to making usual childcare or dependant or carer arrangements. Any arrangements must require to have in place to enable remote working as business hours.

For the purpose of this policy, the term remote working applies equally to remote and mobile working

Applicability of policy

This policy applies to all members of staff (including temporary and contract), partners, and contractual third parties.

- This policy should be adhered to at all times whenever any user makes use of portable computing devices
- The policy also applies to all users who access DMRC information systems or information whilst outside the United Kingdom

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

- Laptop computers
- Tablet PCs
- Mobile phones inc Smart phones
- Text pagers
- Wireless technologies

Computer Equipment

There are several IT solutions to achieving a suitable remote working. Using personal computer equipment will be subject to DMRC connection policies to DMRC's systems and any such computer equipment will be their personal responsible for any repairs or technical support.

Security

DMRC's Information Security Policy must be complied with at all times.

Remote workers shall be responsible for the security of all data, whether held on disc/encrypted memory stick or paper and must ensure it is stored securely to maintain confidentiality of information from anyone.

Sensitive material or personal data must be addressed accordance with DMRC's Cyber Security Policy.

Anti-Virus Protection

Remote working and personal machines will deploy an up-to-date Anti-Virus or other suitable hygiene products. Any Anti-Virus software must be update daily.

Access control

Microsoft Two factor authentication app must be used when accessing DMRCs network and information systems.

As compliance criteria on DMRC become more complex the IT Service may need to apply further security controls from time to time.

Signed

(employer)

Dated: 1 January 2022

Review Date: 31 December 2023

END DOCUMENT