REMOTE AND MOBILE WORKING POLICY

1. Purpose and Scope

This document forms the University of Reading's which supports the

3. Responsibility

3.1 Heads of Schools/Functions/Departments are responsible for ensuring that staff are aware of the need to adhere to this and other related policies when working remotely or on the move and that breaches are dealt with appropriately.

3.2 DTS shall ensure that advice and guidance on technical specifications (such as encryption) is made available to staff.

3.3 Information Asset Owners/Stewards/Custodians:

- Shall ensure that corresponding processes are in place to authorise remote access and mobile working within their area of responsibility.
- Where third-parties have been permitted to access University systems remotely, ensure that appropriate contracts are in place to cover such access, and that said contracts are regularly reviewed to ensure compliance with this and other information security policies.

3.4 University Staff shall:

- Read, understand and comply with this and other related policies.
- Complete all required information compliance training.
- Report the following to DTS:
  - Suspected or actual breaches of this policy.
  - Misuse of mobile devices.
- Report any breaches or suspected breaches of Information Security in accordance with the .

4. Consequences of Non-Compliance

4.1 Failure to comply with this policy may result in:

- Revocation of access to University systems.
- Removal of user rights to University issued mobile devices.
- CoTc 0 Tw 16.12 0 9.295

5.3 Should refrain from storing files locally (on the devices own drive or desktop), particularly if they contain information classified as 'restricted or 'highly restricted' as defined in the _____ _____ Contact DTS or IMPS for more information.

5.4 Should refrain from working on 'restricted' or 'highly restricted' information in public places (unless absolutely necessary to do so).

5.5 Shall never leave papers or equipment containing 'restricted' or 'highly restricted' information unattended outside of University premises unless they are appropriately physically secured from theft in line with University information handling procedures.

5.6 Shall take steps to ensure that the environment offers a suitable level of privacy (i.e. from other individuals in the vicinity being able to view papers or screens being worked on, or being able to overhear private conversations) before working on any 'restricted' or 'highly restricted' information outside of University premises.

5.7

here: http://www.reading.ac.uk/internal/humanresources/WorkingatReading/humres-flexibleworking.aspx