REMOTE AND MOBILE WORKING POLICY

1. Purpose and Scope

This document forms the University of Reading's *Remote and Mobile Working Policy* which supports the *Information Security Policy*. Compliance with this policy will ensure that consistent and appropriate controls are applied to help mitigate the information security risks (detailed below in section 2) associated with remote and mobile working.

1.1 The policy is intended to support the University's aim to enable its staff to work from any location on any appropriate portable device whilst maintaining the confidentiality, integrity and availability of the University's information assets. It is also intended to ensure that third parties working off site apply equivalent protection to the University information that they are handling.

1.2 This policy applies to all University staff accessing university systems and information remotely. It applies to information in all formats, including manual records and electronic data.

1.3 For the purposes of this policy, the terms "mobile" and "remote" are used interchangeably, and should be taken to cover any scenario where University related business is carried out off campus (at home, in a café, another institution, on a train etc.) or outside of the secure University computing environment (this includes working while connected to University Wi-Fi networks).

2. Associated Risks

2.1 *Loss or theft of the device*: Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as University campus locations.

2.2 *Being overlooked*: Some users may work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.

2.3 *Loss of credentials*: If user credentials (such as username/password) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.

2.4 *Unauthorised access to remote gateways*: Credentials that are stolen via other attacks (such as phishing) may be used by attackers to gain unauthorised access to interfaces that are exposed to the Internet, such as email or HR systems. This can potentially compromise any information stored within those systems.

2.5 *Tampering*: An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

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 *Information Security Incident Response Policy*.

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.
- Cost of replacing equipment charged to relevant department/school.
- Action taken against members of staff (including third parties) up to and including dismissal/termination of the engagement.

4.2 The University reserves the right to restrict remote and mobile working if information risks are not being managed in accordance with this, and other University policies.

5. Requirements

Staff working remotely:

5.1 Via an unmanaged device (not University owned/issued) shall do so in accordance with the *Bring Your Own Device Policy*.

5.2 Via a managed device (University owned/issued) shall do so in accordance with the *Mobile Device Management Policy.*

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 *Information Classification Policy*. 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 Shall ensure that any University information or University information asset equipment is appropriately disposed of in accordance with the University's *Information Classification Policy* and *IT Equipment Disposal Policy*.

5.8 Should take precautions when using public or free Wi-Fi services (such as those commonly found in public libraries and coffee shops) to ensure that any sites they visit are genuine. Confidential data (including login details and other business-sensitive information) must not be transmitted or accessed on an unsecured Wi-Fi as it is possible that the information could be viewed by unauthorised individuals.

5.9 Shall do so in accordance with all applicable legislation and shall ensure that all University records and information held remotely or on campus facilities can be retrieved in a reasonable timeframe in the event of an Information Access Request.

5.10 Shall comply with the Payment Card Industry Data Security Standard (for staff handling payment card data). For more information: http://www.reading.ac.uk/internal/finance/fcs-PCICompliance.aspx

5.11 Shall only use approved technologies. End user guidance shall be made available for those engaging in mobile and remote working. This will cover approved technologies and acceptable use.

5.12 Shall ensure that University Information is handled in accordance with the *Encryption Policy* and *Information Classification Policy*, as applicable to the environment in which they are working.

5.13 Shall do so securely, responsibly, and in full compliance with the *IT User Regulations Policy*.

6. Health and Safety

6.1 The University has a duty to protect the health, safety and welfare of their employees and this includes those who regularly work from home. Staff must ensure that their working environment has suitable facilities to effectively carry out their role and shall

ensure that their working arrangements do not unreasonably impact their health and safety.

6.2 Display screen equipment (DSE) advice and guidance is available online (see the *Good Display Screen Equipment Practice* leaflet which covers the core practical needs on breaks, workstation set-up etc.) alongside training, a self-assessment and information on how to contact your local DSE assessor: http://www.cms.rdg.ac.uk/draft/internal/health-and-safety/resources/hs-resources-DSE_Workstation_Assessment.aspx.

6.3 If you wish to vary your working arrangements to work from home for any part of the working week, you can make a formal request for flexible working by following the procedure found here: http://www.reading.ac.uk/internal/humanresources/WorkingatReading/humres-flexibleworking.aspx.

6.4 All incidents that occur on University property, or on University business, that affect staff, students or property must be reported to Health and Safety Services: https://www.reading.ac.uk/internal/health-and-safety/IncidentReportingandEmergencyProcedures/IncidentNotification/

7. Related policies, procedures, guidelines or regulations

7.1 This policy sits beneath the University of Reading's overarching *Information Security Policy*. This and other supporting policies can be found here: http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

7.2 Guidance on remote working: http://www.reading.ac.uk/web/files/imps/DosandDonts-homeworking.pdf

7.3 Health and Safety homepage: http://www.reading.ac.uk/internal/health-and-safety/hs-home-2.aspx

8. Policies superseded by this policy

Remote Working Policy v1.0

9. GLOSSARY

IMPS	means the Information Management and Policy Services department.
DTS	means the Digital Technology Services (IT) department.
Information Asset Owner	means the designated owner of risks associated with specified information assets (IAs), responsible for actioning quality and security controls.
Data Steward	means the designated owner of risks associated with specified Information Asset systems, responsible for data quality within the IA system, providing assurance on quality and security to Information Asset Owners, conducting granular risk assessments and overseeing the implementation of quality and security controls.

Data Custodians	Means the person (s) responsible for the technical environment, for example DTS Support.
Staff	**Includes:** - Employees (including temporary or short term workers) of the University or a subsidiary company of the University. - Volunteers, interns and those undertaking placements or work experience. - Contractors engaged by the University. - Students working for and/or on behalf of the University, including Postgraduate Research students. - Those with University accounts by virtue of a visiting or courtesy title conferred by the University. - Any other individual who is working on behalf of the University if they are processing University data or information.

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
2.0	N/A	DTS	Annually	University Policy Group	MAY 20	MAY 20	MAY 21