Digital Technology Services (DTS)
Information Management and Policy Services (IMPS)

University of Reading

Remote and Mobile Working Policy

1 Purpose

1.1 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 associated with remote and mobile working.

1.2 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.

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

1.4 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 Definitions

Device	Includes – but is not limited to – laptops, computers, netbooks, tablets and smartphones that are used to collect, store, access, transmit, carry, use or hold any University data.
High Risk Data	Defined in the University's Encryption Policy (see Section 7 – High risk personal data or sensitive information) and including any other information which is identified as being of a confidential or proprietary nature.
Personally owned devices	Devices owned, rented or leased by a member of staff.
Processing data	Obtaining, recording, holding, sharing, and retaining and deleting of University data.
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 Post Graduate 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.
Information Asset Owner	The designated owner of risks associated with specified information assets (IAs), responsible for actioning quality and security controls.
Data Steward	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	The person(s) responsible for the technical environment, for example DTS Support.

3 Roles & Responsibilities

University's Cyber & Information Security Group	Implementation, monitoring and review of this policy.
Information Management and Policy Services (IMPS)	Ensuring training, guidance and advice regarding data protection compliance is made available to staff.
Digital Technology Services (DTS)	Ensuring advice and guidance on technical specifications, such as encryption - required under this policy - is made available to staff.
Heads of Schools, Functions and Departments	Ensuring that their staff are made aware of this policy and that breaches of it are dealt with appropriately.
University staff	University staff are responsible for: • Complying with this policy. • Ensuring that their use of personally owned devices is in line with University

	requirements to ensure data security and the protection of University owned intellectual property and confidential information. • Ensuring that no unauthorised persons are able to access University owned data on their personally owned devices. • Ensuring that University data is removed from the device before disposing of the device or selling it or passing onto another individual.
Information Asset Owners/Stewards/Custodians	Ensuring 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.

4 Consequences of Non-compliance

4.1 Failure to comply with this policy may result in us revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

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 Guidance and Key Principles

Associated Risks

5.1 **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.

5.2 **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.

5.3 **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.

5.4 **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.

5.5 **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.

6 Requirements

Staff working remotely:

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

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

6.3 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.

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

6.5 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.

6.6 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. This includes working from home where others may be able to see or hear sensitive information.

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

6.8 Should take precautions when using public Wi-Fi services. Use the University’s VPN service if processing High Risk Data.

6.9 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.

6.10 Shall comply with the Payment Card Industry Data Security Standard (for staff handling payment card data). For more information: PCI DSS Compliance

6.11 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.

6.12 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.

6.13 Shall do so securely, responsibly, and in full compliance with the IT User Regulations and the Information Security Policy.

Health and Safety

6.14 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.

6.15 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: b29462-dse-leaflet-amends-mp-v1-jan-2023.pdf.

6.16 HR have information about Smart Working which covers wellbeing and health and safety when staff sometimes work from home. If you wish to vary your working arrangements to work from home for any part of the working week on a fixed basis, you can make a formal request for Flexible working.

6.17 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

Key related policies and rules:

- Data Protection Policy
- Information Security Policy
- Regulations for the Use of the University of Reading's IT Facilities and Systems
- Encryption Policy (the Policy on Processing Personal Data and Sensitive Information off Campus or on an External Network)
- Remote and Mobile Working Policy
- Mobile Device Management Policy
- Guidance on Remote Working
- Policy on the Acquisition, Use and Transfer of Mobile Telephones
- IT Equipment Disposal Policy
- Code of Practice on Intellectual Property
- Equal Opportunities

- Information Security Incident Response Policy

8 Review

8.1 This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar
- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

8.2 Substantive changes shall be reviewed and approved by the Approving Authority as detailed within Document Control.

8.3 Non-substantive, minor, or administrative changes may be made by the Policy Owner, or representative of the Policy Owner, as detailed within Document control.

9 Policies superseded by this policy

Remote and Mobile Working Policy version 2.1.

10 Document Control

Version	Changes	Keeper	Reviewed	Approving Authority	Next Review
2.0	N/A	DTS	May 20	CUPP	May 21
2.1	Reviewed and links updated	DTS	Nov 21	DTS	Nov 23
2.2	• When using public Wi-Fi, the University's VPN service must be used if processing High Risk Data • Added reference to Smart working	DTS	Dec 25	CUPP	Dec 27