Information Security Remote and Mobile Working Policy

Version Number:	1.1
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Data & Information Management Oversight Group
Effective Date:	19 April 2018
Date of Next Review:	March 2020

1 Purpose of the Policy

1.1 Remote and mobile working is important to the University community and enables flexible working practices. The need for "anytime, anywhere" access to University Information (see ***Definitions*** below) has to be balanced however against the need for an appropriate level of information security.

1.2 This policy is intended to support the University's aim to enable its members to work from any location on any suitable portable device whilst appropriately protecting the confidentiality, integrity and availability of the University's information assets. It is also intended to ensure that third party contractors working off site apply equivalent protection to the University information that they are handling.

2 Scope

2.1 Remote or mobile working comprises working on digital or hard copy University information off site or on the move such as at home, at another institution, in a café, on the train or at a hotel.

2.2 This policy applies to all members of the University and third party contractors.

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and its supporting policies, specifically:

- Information Classification and Handling Policy
- Encryption Policy
- IT Security Baseline Controls Policy

- Data Protection Policy

4 Policy Statement

The University shall deploy appropriate technical and organisational measures to mitigate information security risks associated with remote and mobile working. The University will promote an environment in which information security practices are applied appropriately, consistently and logically across all remote and mobile information handling situations to reduce information-related risk to an acceptable level. Individual members of the University and third party contractors shall take responsibility for ensuring the security of the information they handle remotely via a portable device or from non-University managed premises, in line with the University's requirements.

5 Policy

5.1 When working remotely or on the move University members and third party contractors (hereafter referred to as 'workers') shall ensure that University Information is handled in accordance with the Information Classification and Handling Policy and Procedures, as applicable to the environment in which they are working.

5.2 At all times workers should guard against the possibility of unauthorised access to Classified University Information arising from an unrestricted environment. Specifically:

- Workers should not work on Highly Confidential Information in public places.

- Workers should 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 Classified Information outside of University premises.

- Workers should never leave papers or equipment containing Classified Information unattended outside of University premises unless they are appropriately physically secured from theft in line with the Information Handing Procedures.

- Workers should ensure that any University Information and/or University Information Asset Equipment is disposed of in accordance with the University's Confidential Waste Guidance and/or Secure Disposal of Information Asset Equipment Policy.

- Workers 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 to which they are directed are the genuine sites and, once browsing is finished, to log off any services and tell the device to forget the network.

- Workers should avoid transmitting University Classified Information (including sending their username and password) over an insecure network (e.g. one that does not start with 'https').

5.3 IT Equipment

Workers shall ensure that any IT equipment (including smartphones) used to work on University Information remotely or on the move has been secured according to the relevant provisions of the University's Encryption Policy and the IT Security Baseline Controls Policy.

5.4 Remote Access to University Filestore and Applications

Workers are encouraged to use secure remote access methods of accessing Classified University Information whereby the information is not downloaded on to the remote or mobile device. The currently supported remote access services are listed in Schedule A.

5.5 File Transfer, Synchronisation and Sharing Tools

Workers shall ensure that the use of any file transfer (including email), synchronisation and sharing tool to support remote or mobile working is compliant with the Information Classification and Handling Procedures. In particular workers must not put Classified Information at risk of compromise of confidentiality or critical information at risk of loss through the use of non-secure tools and methods (such as non-approved third party services) and/or personally owned accounts. The currently approved University tools are defined in the Information Handling Procedures.

Workers shall not set up syncing of folders in such a way that Classified Information is stored on non-secured laptops or computer workstations (see the Encryption Policy; IT Security Baseline Controls Policy and the Information Handling Procedures for the required security measures relevant to the device being used).

6 Responsibilities

Heads of Schools/Departments/Colleges are responsible for ensuring that staff are aware of the need to adhere to this policy when working remotely or on the move.

Individual workers (University members and third party contractors) are responsible for adhering to the information security framework policies and following the provisions of this and all related policies. Where the policy requirements are reliant on individual workers taking steps to secure the information they are handling the individual member of workers will be personally accountable and liable for failing to follow the required policy, procedure or process. Individual workers are responsible for ensuring that any shortfalls in baseline security controls are reported promptly to their line manager and (where an incident has occurred) to IT Service Desk.

7 Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary polices or the Student Disciplinary Code as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

Definitions

University Information – any information (in any format) that the University acquires, creates, modifies or stores in connection with its own business purposes.

SCHEDULE A – CURRENTLY APPROVED SECURE REMOTE ACCESS SERVICES

Desktop brokerage services such as Citrix

IT Services VPN

Remote desktop capability

Call the IT Service Desk on 02922 5(11111) for further advice