Remote Working Policy

1 Scope and definitions

1.1 This policy applies to all staff who use or access University systems or information remotely either occasionally or as part of their contract. It applies to information in all formats, including manual records and electronic data.

1.2 'Remote working' means working off campus or outside of the secure University computing environment; this includes working while connected to the University Wi-Fi networks.

1.3 'Staff' includes anyone working on behalf of the University or given access to University data, eg visitors, students and subcontractors.

2 Purpose

2.1 To ensure that staff are aware of their individual responsibilities around information security when working remotely.

2.2 To ensure staff work in accordance with the University's information compliance policies (www.reading.ac.uk/information-compliance-policies).

2.3 To provide policy and guidance for staff on secure remote working and so minimise the risk of unauthorised access to, and loss of, data.

3 Background and risks

3.1 Remote working presents both significant risks and benefits for the University.

3.2 Staff may have remote access to information held on secure campus servers, but without the physical protections available on campus and the network protections provided by firewalls and access controls there are much greater risks of unauthorised access to, and loss or destruction of, data. There are also greater risks posed by information 'in transit'.

3.3 The risks posed by remote working with University information can be summarised under three headings:

- reputational: the loss of trust or damage to the University's relationship with its customers, partners or funders;

- personal: unauthorised loss of, or access to, data could expose staff or students to identity theft, fraud or significant distress; and
- monetary: some regulators, whether in the UK or overseas, can impose penalties of up to £500k.

3.4 This policy sets out policy and guidance on how staff can work remotely in a secure and low risk fashion.

4 Roles and responsibilities

4.1 Any member of staff working remotely is responsible for ensuring that they work securely and protect both information and University-owned equipment from loss, damage or unauthorised access.

4.2 Line managers are responsible for supporting their staff's adherence with this policy.

4.3 Failure to comply with University information compliance policies may result in disciplinary action.

5 Policy statement

Staff working remotely must ensure that they work in a secure and authorised manner as set out in the Key principles below.

6 Key principles

The policy statement in 5 above is underpinned by the following Key principles. All staff must comply with these principles when working remotely.

i. Do not use IT equipment where it can be overlooked by unauthorised persons and do not leave it unattended in public places.
ii. Use automatic lock outs when IT equipment is left unattended.
iii. Ensure that the master copy of the record, whether paper or electronic, is not removed from University premises. In identifying master copies of record, staff should seek advice from their IMPS Contact or the Data Protection Officer.
iv. Where possible, IT equipment must be encrypted in accordance with the standard set out in the University's encryption policy (www.reading.ac.uk/encryption-policy).
v. You should not work remotely if there is a risk to your health or safety, for example during building work at home or in unsanitary conditions, or if there is not a satisfactory work space for you to use. It is the responsibility of the member of staff to ensure that the working environment and space is suitable for remote working.
vi. Before working remotely you must have successfully completed the University's information compliance training (www.reading.ac.uk/information-compliance-training).
vii. Do not use non ITS-authorised ways of working or remote working products, like gotomypc or using internet cafes, when accessing University systems and data. VPN is

the ITS-authorised way of working remotely and any exceptions must be authorised by ITS.

viii. Access to certain systems and services by those working remotely may be deliberately restricted or may require additional authentication methods. Any attempt to bypass these restrictions may lead to disciplinary action.

ix. Staff should be authorised to remotely access University information or systems by an appropriate authority, usually their line manager or Head of School (or equivalent).

x. A risk assessment should be conducted according to the template provided in Appendix 1 before the remote working begins.

xi. When the University provides IT equipment to staff, it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices in the secure office environment. Unlike personally-owned devices which are managed by their owners, University-owned devices will be managed by IT. Staff who have been provided with University-owned IT equipment to work remotely must:

a. only use this equipment for legitimate University purposes;
b. not modify it unless authorised by IT;
c. return the equipment at the end of the remote working arrangement or prior to the recipient leaving the University; and
d. not allow non-staff members (including family and friends) to use the equipment.

xii. Users who process University-held information on privately-owned equipment are responsible for the security of the device and must follow the University's mobile and BYOD policies [link to BYOD].

xiii. Staff working remotely must ensure that information is retrievable. The access to information regimes – freedom of information and data Protection - gives the public rights of access to information held by the University, and this covers information held remotely. In the event of a request for information staff must retrieve *all* relevant requested information, whether held remotely or on campus facilities, and within a reasonable time so that the University can meet the relevant statutory deadlines for responding.

xiv. Staff working remotely must adhere to the University's records retention policy and guidelines, and in particular ensure that information held remotely is managed according to respective School/Service records retention plans and securely deleted or destroyed once it is no longer necessary to process it remotely.

xv. Check the licensing provision for dedicated or specialist software to ensure that it covers remote working, including in the country or region where remote working is to be performed. Further information can be found here:

http://www.reading.ac.uk/internal/its/services/its-SerCat/its-SerCat-Software.aspxand
http://blogs.reading.ac.uk/itsnews/2011/12/06/software-licencing-%e2%80%93-advice-change/

All staff, students and others who work on behalf of the University must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any University-owned IT equipment or data immediately to itsservicedesk@reading.ac.uk, in order that appropriate steps may be taken quickly to protect University data. Failure to do so immediately may seriously compromise University security and, for staff, may lead to investigation and potentially action under the disciplinary procedures.

Version	Keeper	Reviewed	Approved by	Approval date
1.0	IMPS	Annually	ISWG	23/01/15

APPENDIX 1 – Risk assessment

The risk assessment should consider the following:

i the sensitivity of the information to be processed

a. does the information to be process fit the 'high risk' category as defined by the University's encryption policy (www.reading.ac.uk/encryption-policy)?
b. is it sensitive or private in some other way?
c. if 'yes' to either 'a' or 'b', consider working at the University instead of remotely
d. if remote working is the only option, can you access the information you need via a secure mechanism, eg VPN?
e. can you reduce the amount of data you are using and avoid storing any high risk data?
f. is the information encrypted when stored and in transit? If not, it should be.

ii the security of the equipment and system to be used.

a. can the device be encrypted? If so, how are encryption keys, ie passwords, managed?
b. does the equipment comply with the policy and guidance set out in the BYOD and mobile device management policies? [link?]
c. can the device be configured to "auto-wipe"?
d. can you enable remote lock/erase/locate features?
e. has the security of the device been undermined (e.g. by "jail breaking" or "rooting" a smartphone)?
f. can you configure your device not to connect automatically to unknown networks?

iii the suitability of the proposed location for remote working.

a. what is the risk of theft?
b. can devices be left unattended and be secure?
c. how can you protect yourself against "shoulder surfing"?
d. are you using open (unsecured) wireless networks?
e. if a personally owned device needs to be repaired, is the company you use subject to a contractual agreement which guarantees the secure handling of any data stored on the device?
f. is the final exit door secured by a mortice deadlock?
g. Are all other external doors lockable with a secure locking mechanism or security bolts?
h. are your windows lockable while at the same time appropriate in terms of fire safety?
i. can your device or high risk information be locked away when not in use?
j. have you checked with your insurer that your policy covers you for working at home?
k. does the location enable you to work in the most secure way of working in the context, eg VPN?
l. have you done a DSEasy (or equivalent) assessment and ensured that you can work without risk to your health from poor ergonomics ? Please note that the University is not responsible for your remote working environment or desk and screen equipment.

