**University of Manchester – Finance Directorate**

**Working from Home – Data Protection and Related Issues**

All the University’s policies on Data Protection apply when a member of staff takes work home, uses their own devices or accesses University databases from a remote site.

For a general overview, see: <http://www.dataprotection.manchester.ac.uk/>

The Data Protection Office has issued a brief summary of the additional rules applying when working from home:

1. Staff must obtain permission from their line manager to work from home especially if it involves transporting and processing personal data at home. The data protection principles must be maintained at all times and special care should be taken when transporting personal data.
2. Personal data must never be kept on laptops or portable storage (such as USB drives) unless the device or the file has been encrypted. Information on encryption at the University can be found <http://www.itservices.manchester.ac.uk/secure-it/encryption/>
3. If personal data is lost or accidentally disclosed to third parties, this must be reported to the Records Management Office immediately so that remedial action can be taken.
4. Further information, including the forms to report data protection incidents: <http://www.dataprotection.manchester.ac.uk/howdoi/reportadataprotectionincident/>

**Security Rules**

1. Never reveal or share passwords. Do not write them down unless absolutely necessary.
2. Lock your computer or completely log off whenever you leave your workstation; do not rely on the automatic screen lock.
3. Never store personal information on your local drives; use network storage instead.
4. Turn off file and printer sharing on your computer.
5. Any kind of personal data sent by email must be encrypted.
6. Encrypt all sensitive data held on USB drives, CDs or laptops.
7. Immediately report lost or stolen items like laptops, mobiles, USB drives and ID cards through the appropriate channels (see above).
8. Verify the security of online payment systems you use.
9. Limit print outs to information that is not sensitive. Dispose of printouts by shredding.
10. Secure your computer by configuring it to automatically check for software updates - especially up to date antivirus software.

**Other relevant University policies:**

IT Services guidance on working from home:

<http://www.itservices.manchester.ac.uk/our-services/my-it/remoteworking/>

Health and Safety guidance on working from home:

<http://www.healthandsafety.manchester.ac.uk/toolkits/work_off_campus/home_working/>

HR Flexible working policy: <http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=9>

Information Commissioners’ Advice on Bring Your Own Device (BYOD):

<https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf>