Keele University Removable Media Guidance

1. Introduction

1.1 Keele University is committed to preserving the **confidentiality**, **integrity** and **availability** of its data. Data once it is copied onto removable media is immediately put at greater risk of being compromised.

1.2 You are accountable for the security of the data that you store on removable media. Should the removable media containing University data be lost, stolen or the data on it is compromised, this will constitute a breach of the Data Protection Act 1998. In the event of a breach, you will have to demonstrate that your actions leading up to the theft, loss or compromise were reasonable.

1.3 Failure to comply with this guidance may constitute grounds for action under the University's disciplinary procedure.

2. Scope

2.1 This guidance applies to anyone who processes University data including staff, students, visitors and contractors. Removable media includes but is not limited to USB memory sticks, SD cards, SIM cards, external hard drives or any similar storage device.

3. Requirements

3.1 **Do not** store University personal data on unencrypted removable media. For advice on encryption for removable media contact the IT Service Desk. Personal data is any data that can identify an individual.

3.2 **Do not** store on unencrypted removable media any data that if it were compromised could have an adverse effect on the reputation of the University or the ability of the University to function.

3.3 **Do** only copy data to removable media when there is a legitimate and necessary need to do so. Once it is no longer necessary you must completely remove the data from the removable media.

3.4 **Do not** allow access or use of the removable media by unauthorised individuals including friends and family.

3.5 **Do** make sure that you back up the data on the removable media to the University network drives and ensure that a unique copy is not solely stored on the removable media.

3.6 **Do** securely lock away removable media when not in use.

3.7 **Do not** connect a USB device that you find, belongs to someone else or you are unsure of to a device on the University network instead report it to the IT Service Desk.

3.8 **Do** report it to the IT Service Desk immediately if you lose removable media containing personal data even if it is encrypted.

3.9 **Do not** copy personal data to a CD or DVD unless the contents can be encrypted.

3.10 **Do** destroy CDs and DVDs containing personal data immediately once they are no longer needed.

3.11 **Do** store Video and Audio tapes containing personal data that cannot be encrypted in locked cabinets within locked rooms.

3.12 **Do** always ensure that your removable media is virus/malware free before using it on University owned PCs.

4. Contact

4.1 If you require further advice or you are in doubt about any of the contents of this guidance and what is expected of you raise a support call with the IT Service Desk or speak to your line manager.