SOP Title Reference: **RemovMedia**	Last Reviewed: **12/10/2017**	Last Revised: **31/05/2017**	St George's University of London
Author: **IT Services**			

IT Services
IT Policies and Procedures

Removable Media Policy

Contents

1. Policy Statement

SGUL will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official university business.

2. Purpose

The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of SGUL’s computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of ‘protected’ and ‘restricted’ information.
- Prohibit the disclosure of information as may be necessary by law.

3. Scope

This policy applies to all SGUL staff and students, contractual third parties and any other authorised persons who have access to SGUL information, information systems or IT equipment and intend to store any information on removable media devices.

4. Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store University personal data, sensitive personal data (e.g. patient identifiable data), confidential and other business critical information on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

5. Procurement of Removable Media

Only official SGUL removable media devices, i.e. those owned or issued by the University, should be used to store or transfer University personal data, sensitive personal data (e.g. patient identifiable data), confidential and other business critical information.

Non-SGUL owned, e.g. personal, removable media devices **must not** be used to store any information used to conduct official university business.

Technical advice regarding appropriate removable media devices can be obtained by contacting the IT Services Help Desk.

6. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for university purposes is held. Copies of any data stored on removable media should also remain on the source system or be backed up securely to an appropriate network drive.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

Encryption

Personal data, sensitive personal data (e.g. patient identifiable data) confidential and other business critical information must always be encrypted when stored on SGUL removable media.

BitLocker drive encryption can be used to encrypt USB sticks and external hard drives which will help protect files stored on the device. BitLocker is installed as standard as part of the SGUL desktop.

Where data is to be stored on a DVD or CD, 7-Zip can be used to encrypt the individual files. 7-Zip is available on all SGUL machines.

Instructions on how to encrypt using BitLocker and 7-Zip can be found on the IT Training pages in the Portal:

https://portal.sgul.ac.uk/org/lis/computing-services/ittraining/security/security

Further guidance on the secure handling of personal and sensitive personal data can be obtained from the SGUL Data Protection Officer.

7. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to Information Services.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to Information Services.

8. Third Party Access to University Information

No third party (external contractors, partners, agents, the public or other non-employee parties) should receive data or extract information from the SGUL network, information stores or IT equipment without explicit agreement from an authorised member of SGUL staff.

Should third parties be allowed access to university information then all the considerations of this policy apply to their storing and transferring of the data.

9. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact Information Services should removable media be damaged.

Virus and malware checking software approved by the Information Services must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to SGUL, other organisations or individuals from the data being lost whilst in transit or storage (see section 6. ‘Encryption’)

10. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the university or for personal use, must be erased.

This must involve a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to IT Services for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the IT Services Help Desk.

11. User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- All data stored on removable media devices **must** be encrypted where personal data, sensitive personal data, confidential or business critical information is involved.

- Virus and malware checking software **must** be used when the removable media device is connected to a machine.

- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment.

- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

For advice or assistance on how to securely use removable media devices, please contact the IT Services Help Desk.

12. Policy Compliance

If any user is found to have breached this policy, they may be subject to SGUL’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the department of IT Services.