Data Management Guidance

2 March 2017

Purpose

The policy provides a basis for data management at PSSRU.

General information Security

1. Always comply with the Data Protection Act (DPA) 1998[1] and data sharing agreements (DSAs).
2. Project managers will have responsibility for ensuring that appropriate security measures are in place for their team. Principal investigators (PIs) will discuss data security at the beginning of the project.
3. All researchers are responsible for the security and protection of data.
4. Laptops and offices should always be locked when not in use.
5. Researchers are required to report any loss of data to the Computing Manager and the project's PI.
6. Staff will be required to complete the ECDL module 1 (IT Security).
7. Staff who have access to data will be asked to complete a data security form.
8. Researchers should seek advice from the Computing Manager if they are unclear about any aspect of data security.

Assume that data security is relevant to you

General data storage and use

1. Personal data[2] (i.e. data about an individual) should be encrypted at all times when not in use and should not be available offline.
2. All data should be stored on university network servers.
3. No data should be stored on removable media such as CDs, memory cards, USB flash drives, including external disk drives, unless approval from the PI has been granted. In this case, data can ***only*** be stored on encrypted devices.
4. Sharing of data across project teams is not allowed unless you have consent from the participant to do so and the process has been approved by the appropriate ethics committee.
5. At the end of projects, researchers should review the content of files and securely shred unwanted data. The Computing Manager will arrange data destruction. If arrangements have been made to retain data for a set period after the project has ended, procedures should be in place to review the storage of that data periodically.

HSCIC data process and storage

1. PSSRU Executive Group (EG) have overall responsibility for the data and DSAs.

[1] https://www.gov.uk/data-protection/the-data-protection-act

[2] https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

2. Staff will be required to submit a request to the Data Management Group (DMG) outlining why they should have access to HSCIC data. DMG will provide access if it is required.
3. HSCIC data will be encrypted at all times when not in use and will not be available offline.
4. No copies of HSCIC data will be allowed outside the designated folder. If datasets are found outside the folder, they will be destroyed without warning.