St George's, University of London
Data Safe Haven Policy

1 Purpose

1.1 The purpose of this document is to provide a clear statement to researchers of St George's, University of London regarding the management of its Data Safe Haven (DASH).

1.2 The policy constitutes part of the Information Governance Framework and should be read alongside applicable University research policies and procedures.

2 Scope

2.1 This policy covers all research projects which DASH supports and applicable to all personal within scope of the DASH.

3 New Users

3.1 Access

3.1.1 The DASH is accessed using unique credentials that are independent to standard University network credentials.

3.1.2 To access the DASH you will need to submit the 'Account Request' form. The request must be authorised by the Principal Investigator (PI) or Information Asset Owner.

3.1.3 New users must have completed the appropriate information governance training prior to being issued with an account. You will be asked to confirm you have done this, and to indicate that you agree to abide by all the relevant University policies.

3.1.4 Once your account request has been approved you will have to collect your credentials in person. They cannot be sent out to you.

3.2 Accessing resources

3.2.1 If you would like to set up a new share within the DASH you must complete the 'New Share Request' form.

3.2.2 If you need to be able to access existing research folders, i.e. data already in the DASH, you will need to ask the owner of that share to complete the 'Add New or Remove Existing User Request' form.

Existing Users

3.3 If you already have an account for the DASH and would like to request additional resources, or make changes to existing resources, you will need to submit the relevant request form.

3.4 New shares

3.4.1 To request the creation of a new share within the DASH you must complete the 'New Share Request' form.

3.5 Access to existing shares

3.5.1 If you need to make changes to who can access a share that you own you must complete the 'Add New or Remove Existing User Request' form.

3.5.2 If you want to be able to access a share owned by another user, you must ask them to complete the 'Add New or Remove Existing User Request' form for you. Requests will only be accepted from the share owner.

3.6 Changes to existing shares

3.6.1 In order to make any changes to existing shares you must complete the 'Request for Action on a Share' form.

3.6.2 This form allows you to request a change to the share name, and to request that data be deleted, restored, archived or exported. Requests for changes will only be accepted from the share owner.

4 Acceptable use of DASH

4.1 The DASH may be used for authorised University business which involves the processing of sensitive personal data.

4.2 All DASH users are responsible for ensuring the physical security of the environment they work in while working with data held within DASH.

4.3 All use of the DASH must comply with the University policies listed here:

- IT Conditions of Use: Core regulations
- Data Protection Policy
- Information Security Policy
- Technical Security Policy

5 Unacceptable use of DASH

5.1 DASH may not be used for any of the following:

5.2 The creation or transmission, or any other form of processing as defined by UK Data Protection regulations, that is detrimental to the legitimate rights of individuals or likely to cause annoyance, inconvenience or needless anxiety. For the avoidance of doubt this includes but is not limited to the processing of racist, pornographic, sexist or terrorist materials.

5.3 The transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks.

5.4 Non-healthcare profit making activity that grossly abuses the service.

5.5 Other activities that do not benefit patient care or that do not support the professional concerns of those providing that care, where those activities constitute gross abuse of the service.

5.6 Gross abuse of the service by the unsolicited sending of inappropriate e-mail to large numbers of people.

5.7 Deliberate unauthorised access to facilities or services accessible via the DASH.

5.8 Deliberate activities with any of the following characteristics:

Flagrant wasting of staff effort or networked resources, through inappropriate and unauthorised use of DASH facilities including but not limited to the following:

- Corrupting or destroying other users' data;
- Violating the consent, or wishes of data subjects in respect of processing personal or sensitive data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using DASH in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- Continuing to use an item of networking software or hardware after the Head of IT Services has requested that use cease because it is causing disruption to the correct functioning of DASH;
- Other misuse of DASH or networked resources, such as the introduction of "viruses";
- Where DASH is being used to transfer data to another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of DASH.

Note that this list is not exhaustive, and will be updated in the light of experience.

5.9 If you are in doubt about whether you may use DASH for a particular purpose, you should seek advice from itav@sgul.ac.uk.

5.10 It is not permitted to provide access to DASH by third parties without the prior agreement of Director of Information Services or their delegated representative Head of IT Services.

6 Controls

6.1 Ownership of this Policy is with Head of IT Services.

6.2 Responsibility for staff compliance with this policy is with Information Governance Steering Group

6.3 Staff will be made aware of this policy upon publication and on a regular basis afterwards through University internal communications channels, including the University's website Georges Weekly and team briefings.

6.4 New staff will be informed of the policy through the induction process.

7 Assurance

7.1 This Policy will be reviewed every 3 years unless changes are required and will be reported on to the Information Governance Steering Group.